Employee Privacy Policy

Document Control Information			
Version	1.0	Author	GDPRLocal
Reviewer	Signify Technology Group Ltd.	Review Date	01/10/2025
Review Frequency	12 months	Next Review Date	10/2026

The current version of this document is up to date. Any future versions or changes to this document must also be approved by the author and the Executive Team and issued on a version-controlled basis under their signature. This document has been stored at Safe Storage.

Aim

The primary aim of this Employee Privacy Policy is to establish a clear and comprehensive framework that governs the collection, use, storage, and protection of personal data belonging to our employees. Recognising the importance of privacy and the sensitivity of personal information, we are committed to ensuring that all personal data is handled with the utmost care and in accordance with relevant data protection regulations. This policy serves to inform employees about their rights concerning their personal data, the purposes for which their data is processed, and the measures in place to safeguard their privacy. By setting forth these guidelines, we aim to foster a culture of transparency and trust, ensuring that every employee's privacy is respected and protected within our organisation.

Scope

This Employee Privacy Policy applies to a wide range of individuals or entities associated with our organisation, including but not limited to:

- Associates and/or other individuals engaged - Members affiliated with Signify Technology Group Ltd, specialising in culture-driven consulting and strategy implementation for global organisations.
- Employees - Full-time, part-time, temporary, and permanent staff members who are directly employed by the company;
- Consultants - External professionals who provide expert advice and services on a contractual basis;
- Contractors - Individuals or entities that undertake contractual work for the company, which can range from short-term projects to long-term engagements;
- Interns - Students or recent graduates who work temporarily to gain practical experience in a particular industry or field;
- Volunteers - Individuals who offer their time and skills without expecting monetary compensation;
- Freelancers - Professionals who are self-employed and provide services to the company on a per-project basis.

Introduction

At Signify Technology Group Ltd, we deeply value the trust and confidence our employees place in us, especially when it comes to the protection of their personal information. Recognising the significance of this responsibility, we have established this Employee Privacy Policy to articulate our steadfast commitment to safeguarding the personal data of our employees. This policy outlines the principles and practices we adhere to in collecting, using, storing, and disclosing personal data, ensuring that we operate in full compliance with prevailing data protection regulations and best practices. As we navigate the complexities of the modern workplace, it is our priority to ensure that every employee's privacy rights are upheld and their data is treated with the care and respect it deserves.

Definitions

The General Data Protection Regulations/GDPR - Whenever the terms 'The General Data Protection Regulations' or 'GDPR' are referred to in this document, it usually 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, regardless of where the processing occurs, as well as entities outside the EU 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 [personal data] - 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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.

Processing - Any operation or set of operations performed on personal data, whether or not by automated means. This includes collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

Third-Party/Vendor - A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Instructions on How to Use the Employee Privacy Policy

Familiarise Yourself:

Begin by reading the Employee Privacy Policy in its entirety to understand the scope and purpose. This will provide you with a comprehensive overview of how your personal data is managed within the organisation.

Refer Regularly:

Whenever you're in doubt about any data-related activity or decision in your role, refer back to this policy. It serves as a guiding document for all matters related to employee data privacy.

Stay Updated:

Periodically, the policy may be updated to reflect changes in data protection laws or organisational practices. Ensure you're aware of the latest version and any amendments made.

Seek Clarification:

If any section of the policy seems unclear or ambiguous, don't hesitate to reach out to Data Protection Lead Lauren Palmer, gdpr@signify-tech.com.

Report Concerns:

If you believe there's a discrepancy between the policy and actual practices, or if you identify potential breaches, report them immediately to the appropriate internal channels. Your proactive approach can help in ensuring compliance and addressing issues promptly.

Integrate into Daily Operations:

If your role involves handling personal data of colleagues or making decisions that impact data privacy, always use this policy as a reference point. Ensure that your actions align with the guidelines set forth.

Training and Workshops:

Attend any training sessions or workshops related to the Employee Privacy Policy. These sessions will offer deeper insights, practical examples, and a chance to discuss queries with experts.

Share and Educate:

If you're in a managerial or supervisory role, ensure that your team members are also aware of the policy. Encourage open discussions and ensure that everyone understands its importance.

Safe Storage:

Keep a printed copy of the policy in an easily accessible place, and bookmark the digital version

on your computer for quick reference.

Feedback Loop:

If you have suggestions or feedback about the policy or its implementation, share them with the organization. Continuous improvement is vital for the effectiveness and relevance of such policies.

Remember, the Employee Privacy Policy is not just a document but a commitment to ensuring the privacy and protection of personal data within the organisation. Using it effectively ensures a safer, more compliant, and more transparent work environment for all.

Employee Privacy Notice

How your information will be used

Signify Technology Group Ltd takes the privacy and security of your personal data very seriously.

As an employee, worker, volunteer, consultant, intern, associate, and/or other individual engaged or in any relationship where we are effectively your employer and/or contractor (hereafter you are referred to as an employee) the Company needs to keep and process information about you for normal employment, business operation, and management purposes. This notice describes how we treat your personal data as an employee, how we ensure we meet our obligations to you, and how we endeavour to meet our obligations under the GDPR. We may update this notice at any time, and we may provide you with an additional privacy notice from time to time.

As a consultant, contractor, associate, and/or other individuals engaged, your personal and professional information will be used to facilitate our collaborative efforts in driving organisational culture. This includes understanding your expertise, aligning it with our projects, and ensuring seamless communication and collaboration. Your data will also be used for administrative purposes, project management, and to uphold our commitment to providing the best culture consulting services. We respect your privacy and will handle your information with the utmost confidentiality, adhering to GDPR and other relevant data protection regulations.

The information we hold and process will be used for our management and administrative use only. We will store and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends, and after you have left. This includes using information to enable us to comply with our employment contract, to comply with any legal requirements, pursue the legitimate interests of the company and protect our legal position in the event of legal proceedings.

If you do not provide the personal data requested, we may be unable in some circumstances to comply with our obligations, and we will tell you about the implications of that decision. In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Once you are no longer an employee of the company, we will retain your information for a period of time and then securely destroy your personal information in accordance with our GDPR policy and applicable laws and regulations.

Our Lawful Basis For Processing Your Personal Data

As your employer or contractor, we will normally have your consent to process your personal data, in some situations we have a legal obligation or in extreme situations for example a medical emergency we may be relying on vital interest to process your data however as a company, we may sometimes need to process your data to pursue our legitimate business interests, for example to run our business, prevent fraud, for administrative purposes or reporting potential crimes. We will never willingly process your data where these interests are overridden by your own interests. We aim to process your personal data lawfully, fairly, and in a transparent way.

Our commitment to you as an employee [as a data subject] includes the following:

- To collect your personal data only for valid purposes that we have advised you about and not to use your personal data in any way that is incompatible with those purposes (unless we have notified you and explained the lawful ground that allows us to do so);
- To only process your personal data to the extent necessary for the purposes we have advised you about, or where we believe the new purpose is compatible with the original purpose;
- To ensure we always have a lawful basis for processing your personal data;
- To keep your personal data accurate and up to date;
- To keep your personal data only as long as necessary for the purposes we have told you about;
- To keep your personal data secure;
- To respond promptly and professionally to any request;
- To comply at all times with applicable data protection regulations.

Most of the information we hold will have been provided by you. However, some may come from other internal sources, such as managers and colleagues, or in some cases, external sources, such as referees, social media, recruitment companies, consultants, and other third-party sources. We may from time to time use other sources as required to run our business, protect our interests, and ensure we are able to meet our obligations to you and our customers.

We may collect, store, and use the following categories of personal data about you:

Personal contact details such as name, title, date of birth, gender, addresses, telephone numbers, and personal email addresses;

- Marital status and dependents;
- Next of kin and emergency contact information;

- Bank account details, payroll records, and tax status information;
- Salary, annual leave, pension, and benefits information, national insurance number;
- Medical information relating to medical conditions, tests, treatments etc… ;
- Location of employment or workplace and start date;
- Copy of driving licence/passport;
- Recruitment information (including copies of right-to-work documentation, references and other information included in a CV or cover letter or as part of the application process);
- Employment records (including job titles, work history, working hours, training records and professional memberships);
- Details of your existing and previous salary;
- Performance information and disciplinary and grievance information;
- CCTV footage and other information obtained through electronic means such as electronic key card records;
- Information about your use of our information and communications systems including tracking applications installed on your devices;
- Information collected from tracking and activity tracking software installed on our devices;
- Medical information provided by you or provided to us by third parties including medical conditions, symptoms, medications, the result of tests, treatments, and other consultations.
- Data related to any disabilities or accommodations
- Reports provided by your managers, colleagues, customers, suppliers, and other third parties. We may need to keep the content of these reports confidential;
- Voice recordings/Photographs/Video/Other images and representations;
- CCTV information,
- Other security-related information we may collect about you,
- ID passes;
- Other information as you would reasonably expect in relation to an employee/employer relationship.

We understand that some of this information is considered sensitive under the GDPR. We ensure that we have taken every measure and exercised all reasonable care to protect your personal information. We protect your personal information with utmost care.

Purposes For Which We Process Your Personal Data

We will process your personal data for the following purposes:

- establishing an employment relationship;
- exercising rights and obligations from an employment relationship;
- complying with legal requirements in the field of employment, social security and equal opportunities

The sort of information we hold includes, but is not limited to, your application form and references, your contract of employment and any amendments to it, correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary, information needed for payroll, benefits and expenses purposes, contact and emergency contact details, records of holiday, sickness and other absence, information needed for equal opportunities monitoring policy and records relating to your career history, such as training records, appraisals, other performance measures and where appropriate, disciplinary and grievance records.

Inevitably, you may, be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company.

Your image (photos, voice and videos) may also be used by the organisation on our website, advertising and promotion material, staff and customer newsletters, noticeboards, social media sites and in other areas. Agreeing to this policy is your consent to the use of your image by the organisation. Your image may be used in such material after you have left the company for an indefinite period. If you object to your image being used or would like your image to be removed after you have left our organisation, please inform us directly. Where possible, we will remove your image however it may not be possible to remove your image from material that is in the public domain.

Where necessary, we may keep information relating to your health that could include reasons for absence and GP or other medical reports and notes. This information will be used in order to comply with our company health and safety and occupational health obligations, to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay.

Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation etc., we will always endeavour to obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency, or where collecting your consent would undermine the purpose for which the data was collected. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

In addition, we monitor computer/tablet (and telephone/mobile telephone) use. This includes work activity and any personal activity you undertake on the device as detailed in our Information Security Policy, available (in the company handbook/on the intranet). We also keep records of your hours of work by way of our clocking on and off system, as detailed in the company handbook/intranet.

Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so, where we have a legitimate interest, or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to [external payroll provider], pension or health insurance schemes.

We may transfer information about you to other related companies for purposes connected with your employment or the management of the company's business.

Where your information is transferred internationally, we will ensure we have appropriate safeguards in place to protect your data.

We may use automated decision-making, including profiling, in limited circumstances. Signing this agreement is your consent to the use of this automated processing.

We may use machine learning, AI technology, and other advanced technologies to process your data. Signing this agreement is your consent to the use of this type of processing.

In normal circumstances, your personal data will be stored for a period of up to 7 years after you leave the company unless we determine that we need to retain your data for a longer period.

If in the future we intend to process your personal data for a purpose other than that for which it was collected, we will provide you with information on that purpose and any other relevant information.

Your Rights

Under the General Data Protection Regulation (GDPR), you have a number of rights with regard to your personal data

- **Request access** to your personal information (commonly known as a "Data Subject Access Request - DSAR"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below);
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes;
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example, if you want us to establish its accuracy or the reason for processing it;
- **Request the transfer** of your personal information to another party;
- **Other Requests** - we will respect your rights and respond to any request promptly and professionally.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact gdpr@signify-tech.com in writing. However, we may reject your request for access if it is clearly unfounded or excessive. Where this is the case, we will let you know why we have made this decision.

Review, verification, correction, and erasure of photos, videos, and other images will also be considered where feasible and reasonable. Photos [etc..] which are in the public domain, on social media, on printed material may be impossible or unreasonably difficult to erase. You will not normally have to pay a fee to access your personal data or to exercise any of the other rights under data protection laws. However, we may reject your request for access if it is clearly unfounded or excessive. Where this is the case, we will let you know why we have made this decision.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is

another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

If you believe that we have not complied with the requirements of the GDPR with regard to your personal data you have the right to lodge a complaint with your local Data Protection Regulator. To see the list of Regulators in each country please contact the company visit: https://edpb.europa.eu/about-edpb/about-edpb/members_en

Identity and contact details:

Signify Technology Group Ltd is the controller of your data for the purposes of the GDPR. If you have any concerns as to how your data is processed, you can contact:

Name of Data Protection Lead: Lauren Palmer
Company name: Signify Technology Ltd's
Data Protection Lead email: gdpr@signify-tech.com
Data Protection Lead Address: First Floor, 3 Moorgate Place, London, EC2R 6EA
Data Protection Lead Number: +44 (0)203 865 0621

Or you can write to this individual using the address of Signify Technology Group Ltd

To be signed by the Employee:

I agree to the terms of this Employee Privacy policy.

Signed by Employee (data subject) _____

Date _____

Appendix 1 - California Privacy Laws: CCPA/CPRA

This Annex provides a summary of California employee privacy rights under the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA). This Appendix applies to Signify Technology Group Inc. and may be expanded to include additional US state privacy frameworks as they evolve.

Scope

This Annex applies to personal information collected from California employees, job applicants, contractors, and similar individuals. It supplements the Employee Privacy Policy and outlines specific California rights and obligations.

Categories of Personal Information Collected

We may collect, store, and use the following categories of personal information about you:

Personal and Contact Information

- Name, title, date of birth, gender, addresses, telephone numbers, personal email addresses
- Marital status, dependents, next of kin, and emergency contact information

Employment and Professional Information

- Job title, work history, start date, workplace location, working hours
- Training records, professional memberships, performance information, disciplinary or grievance records
- Salary, benefits, annual leave, pension, tax status, national insurance number, and previous salary details
- Recruitment information, including CVs, cover letters, references, right-to-work documentation, and application materials

Financial Information

- Bank account details, payroll records, and tax-related information

Medical and Health Information

- Medical conditions, symptoms, treatments, test results, medications, consultations
- Disabilities or accommodations
- Allergies, dietary requirements, and other health-related information voluntarily provided

Identity and Verification Documents

Copies of driving licenses, passports, and ID passes

IT and Communication Usage

Information about your use of company information and communications systems

Data collected from tracking or activity monitoring software installed on company devices

Security and Surveillance Information

CCTV footage and other security-related information

Electronic key card records or other device-generated access data

Media and Representations

Voice recordings, photographs, video, or other images and representations

Reports and Feedback

Reports provided by managers, colleagues, customers, suppliers, or other third parties (which may be confidential)

Other Relevant Employee Information

Any other information reasonably expected in the context of the employee/employer relationship

Personal short-term or long-term goals voluntarily provided by the employee

Purposes of Processing

We may collect, store, and use personal information for the following purposes:

1. **Recruiting, Hiring, and Onboarding**
    - To evaluate applications, verify qualifications, conduct background checks, and facilitate onboarding.
2. **Payroll, Benefits, and Tax Administration**
    - To manage salary, pensions, benefits, tax reporting, and related financial obligations.
3. **Employee Performance, Training, and Career Development**

- To evaluate performance, provide feedback, administer training, and support professional growth.

4. **Workplace Safety and Compliance**

   - To ensure a safe working environment and comply with health, safety, and regulatory obligations.

5. **IT Security, Fraud Prevention, and Policy Enforcement**

   - To protect company systems, monitor network activity, prevent fraud, and enforce internal policies.

6. **Compliance with Legal and Contractual Obligations**

   - To comply with laws, regulations, and contractual duties relating to employment.

Sensitive Personal Information: Any sensitive personal information (such as health data, government IDs, or financial credentials) is used only for legitimate employment-related purposes and handled with additional care and confidentiality.

Disclosure of Personal Information

As described in our Employee Privacy Policy, we may disclose personal information about you to the following categories of third parties:

1. **Service Providers:** External payroll processors, benefits providers, pension and health insurance schemes, IT vendors, and background check providers.

2. **Government Authorities:** As legally required, for example for tax, social security, or other statutory reporting obligations.

3. **Professional Advisors:** Legal counsel, auditors, or other advisors who assist us in managing legal, financial, or operational obligations.

Important: We do not sell or share employee personal information for commercial purposes. Disclosures are limited to the purposes described above, including compliance with legal obligations, legitimate business interests, and contractual duties.

Retention of Personal Information

Personal information is retained only as long as reasonably necessary or required by law. Please see our Retention Policy for more information.

Employee Rights under CCPA/CPRA

California employees have the following rights:

Right to know/access: Request the categories or specific personal information collected.
Right to delete: Request deletion of personal information, subject to legal exceptions.
Right to correct: Request correction of inaccurate personal information.
Right to limit use of sensitive information: Limit use or disclosure of sensitive personal information.
Right to opt-out of sale/sharing: Not applicable, as employee data is not sold or shared.
Right to non-discrimination: No retaliation for exercising privacy rights.

How to Exercise Your Rights

Submit requests via:

Email: gdpr@signify-tech.com
Phone: +44 (0)203 865 0621
HR contact: Samantha Smylie [Samantha.smylie@signify-tech.com]

Verification of identity may be required before processing requests.

Contact Information

For questions regarding this Annex or California privacy rights, contact:

Name of Data Protection Lead: Lauren Palmer
Company name: Signify Technology Inc
Data Protection Lead email: gdpr@signify-tech.com
Data Protection Lead Address: 2834 Colorado Ave, Suite 305, Santa Monica, CA 90404, United States of America

Appendix 2 - GDPR Checklist for Employers

Examine this checklist to ensure you've gone through your contracts and related documents, incorporating the necessary privacy notices and consent forms.

Action		Comments	Completed
EMPLOYEE INFORMATION AUDIT			
1.	Identify what personal data you hold about employees and candidates (and where it came from)		
2.	Identify all the ways in which you process personal data and the purposes of the processing		
3.	Verify how long you currently retain the personal data and how long you need to keep the personal data for the purpose for which it is collected		
4.	Identify any parties to whom you transfer personal data, including any international data transfers, for example, payroll and benefits providers and other group entities		
5.	Review any associated contracts		
6.	Identify any automated decision-making within HR processes, for example, in recruitment (automated rejection and short-listing), triggers for sickness absence or disciplinary action, attendance bonuses, shift and holiday roster, and employee monitoring		
7.	Ensure the audit is properly documented		
Identify lawful basis for processing employee personal data under current data protection laws			
8.	This will likely be employee consent, possibly obtained via a clause in the employment contract	(NOTE: it is UNLIKELY to be consent under GDPR)	
9.	Confirm current basis for processing "sensitive personal data" (including details of criminal convictions and offences)		
10.	***Identify lawful basis for processing employee personal data under GDPR. One of the following must apply:***		
10.1	The employee gives valid consent (NOTE that for most purposes consent will not be deemed freely		

Action		Comments	Completed
	given due to the imbalance of power in the employer/employee relationship but it might be appropriate for things like surveys)		
10.2	Necessary to carry out the employment contract (e.g. taking financial data so you can pay them in special leave/benefits)		
10.3	Necessary for the employer to comply with a legal obligation (e.g. taking social security data so that you can pay employer taxes, TU fees)		
10.4	Necessary to protect the vital interests of the employee or another person (e.g. to protect physical/mental health/disability status. To monitor sickness absences/fitness for work)		
10.5	Necessary in the public interest or if the employer is exercising official authority		
10.6	Necessary for a legitimate interest of the employer or a third party which is not overridden by the interests or fundamental rights and freedoms of the employee		
11.	***Identify lawful basis for processing special categories of employee personal data (sensitive data) under GDPR. One of the following must apply:***		
11.1	Valid explicit employee consent		
11.2	Necessary for carrying out employment rights and obligations, it is authorised by domestic law and the employer has an appropriate policy document in place		
11.3	Necessary to protect the vital interests of the employee or another person where the employee is incapable of giving consent		
11.4	Processing by a foundation, association or not-for-profit with a political, philosophical, religious or trade union aim		
11.5	If the employee has made the personal data public		
11.6	Necessary for the employer to establish or defend legal claims		
11.7	Necessary for reasons of substantial public interest (including the processing of personal data revealing		

Action		Comments	Completed
	race, religious beliefs, health or sexual orientation for the purposes of promoting equality of treatment, and including processing necessary to determine eligibility for or benefits payable under an occupational pension scheme which can reasonably be carried out without the employee's consent), and the employer has an appropriate policy document in place		
11.8	Necessary for the assessment of the employee's working capacity either on the basis of applicable laws or pursuant to a contract with a health professional, and subject to confidentiality safeguards		
12.	***Identify lawful basis for processing of employee personal data relating to criminal convictions and offences under GDPR***		
12.1	The processing must be authorised by domestic law and, if authorised by applicable laws, one of the following must apply: Necessary for carrying out employment rights and obligations and the employer has an appropriate policy document in place		
12.2	Valid employee consent (although consent will not be valid where there is a clear imbalance between the data subject and data controller, such as in an employment context)		
12.3	Necessary to protect the vital interests of the employee or another person where the employee is incapable of giving consent		
12.4	Processing by a foundation, association or not-for-profit with a political, philosophical, religious or trade union aim		
12.5	If the employee has made the personal data public		
12.6	Necessary for the employer to establish or defend legal claims		
Data cleansing			
13.	Update data retention policy based on results of audit and apply it (see the data retention policy in the pack)		

Action		Comments	Completed
14.	Securely delete or de-personalise all employee personal data where there is no lawful basis for the processing under GDPR		
Amend HR policies and processes			
15.	For example, procedures relating to recruitment, promotions, compensation, disciplinary, grievances, performance management, sickness absence, employee monitoring and references, conduct a data protection impact assessment (DPIA) if required		
16.	Notify employees of changes to policies/handbook		
Automated decision-making (including profiling)			
17.	Identify the lawful basis allowing you to make decisions that significantly affect an employee based on automated processing:		
18.	Necessary to carry out the employment contract		
19.	The employer notifies the employee in writing of a decision based on automated processing and allows the employee the right to request a reconsideration within 21 days		
20.	Valid explicit employee consent		
21.	Ensure that suitable measures to safeguard the employee's rights and freedoms and legitimate interests are in place, including the right to obtain human intervention, the right to express the employee's point of view and the right to appeal any automated decision		
22.	Automated decision-making on the basis of special categories of personal data must be permitted by valid, explicit employee consent or in the substantial public interest, with suitable measures to safeguard the employee's rights and freedoms and legitimate interests		
Data transfers to third parties (other group entities and service providers)			
23.	Identify lawful basis for all data transfers, including in particular any cross-border data transfers		
24.	Put processor agreements in place where		

Action		Comments	Completed
	necessary		
25.	Update procedures so that GDPR compliance forms part of due diligence when entering into a new contract with an HR supplier		
Notify employees of the processing of personal data			
26.	Draft new privacy notice for employees (use employee privacy notice not the website privacy notice)		
27.	Ensure that procedures are updated so that the privacy notice is provided to employees and candidates when required as future personal data is collected or when the purpose of processing changes		
Data subject rights			
28.	Update SAR policy and procedures: new timeline, free of charge unless request is manifestly unfounded or excessive, new information requirements		
29.	Arrange updated training for all staff who handle SARs		
30.	Establish procedures for dealing with the exercise of employee rights		
Data protection officer (DPO)			
31.	Establish whether you are required to appoint a DPO		
32.	If so, appoint a DPO, scope the role in accordance with GDPR requirements and provide them with the necessary training and resources		
33.	If a DPO is not mandatory, consider designating a senior individual as having responsibility for data protection		
Training and review			
34.	Arrange updated training for all staff who handle personal data		
35.	Ensure that all arrangements and privacy notice are		

Action		Comments	Completed
	subject to regular review for continued compliance		
36.	Ensure any policy document relating to the processing of special categories of personal data or criminal convictions is subject to regular review and updated where appropriate		

Appendix 3 - Consent Statement Example:

Dear [name of employee],

As part of your relationship as an employee, volunteer, contractor, intern, third party, or in any other relationship with this company we may collect, store, and process personal details about you, your next of kin, your employment history, medical condition, photos, images, videos, and other personal information as described in the privacy policy stored in SharePoint and as you would expect in an employer/employee relationship. We will not share your information other than as described in the privacy policy and as you would reasonably expect. We will collect, store, process, maintain, and then delete your data as described.

We respect all your rights under the GDPR and will always respond to requests to withdraw consent, forget your details, correct your details, stop processing or port your data as requested and where feasible.

Important: You can object to processing, and opt to withdraw or amend your consent at any time, simply contact:

Name of Data Protection Lead: Lauren Palmer
Company name: Signify Technology Ltd
Data Protection Lead email: gdpr@signify-tech.com
Data Protection Lead Address: First Floor, 3 Moorgate Place, London, EC2R 6EA
Data Protection Lead Number: +44 (0)203 865 0621

Our Employee Privacy Policy describes exactly how we collect, process, and store your information. This is an important document, and you should take time to read it. Please sign and date below to confirm that you have received and understand the privacy statement.

Signed _____ Date _____

Governance of this document

Our organization views data protection as a critical component of our overall security and privacy strategy. This policy is overseen and owned by our Data Protection Lead (DPL). This key document emphasizes the paramount importance of data in the digital era, mandating a review and update every 12 months by the DPL to ensure continued relevance and compliance. Breaches or non-compliance should be promptly reported to the DPL, highlighting our steadfast commitment to safeguarding our stakeholders' interests.

End.