

# HR DATA PRIVACY NOTICE

1 September 2024

## 1. WHAT IS THE PURPOSE OF THIS DOCUMENT?

Sodexo is committed to protecting the privacy and security of your personal information.

This privacy notice (also referred to as a “privacy statement” in the Global Data Protection Policy) describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the (UK) General Data Protection Regulation (GDPR).

It applies to all current and former employees, workers, and contractors.

For this notice, the Sodexo entity which employs or contracts with you is the Data Controller, this will be:

**Sodexo Limited** of One Southampton Row, London WC1B 5HA

**Sodexo Live UK Limited** of One Southampton Row, London, WC1B 5HA

**Sodexo Remote Sites Scotland Ltd** of The Exchange 62 Market Street Aberdeen AB11 5PJ

**Sodexo Global Services Ltd** of One Southampton Row, London WC1B 5HA

**Sodexo Ireland Ltd** of Fourth floor, One Grand Parade, Dublin 6, D06 R9X8

**Heritage Portfolio Ltd** of 49A North Fort Street, Edinburgh, EH6 4HJ

The entity is referred to as Sodexo in this Notice. This Notice also applies where we manage staff on behalf of clients and where applicable to agency staff.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with Data Protection Law.

The Data Controller is part of the Sodexo Group of companies. Sodexo was founded in France and has developed into an international company operating in 80 countries worldwide. Your Personal Data may be shared with Sodexo entities within the UK or EEA where joint services are provided, for example, HR, payroll, legal and IT. You can find out more about the Sodexo Group by visiting our website. Sodexo Ltd also acts as a Data Controller for Sodexo Live UK Limited, Sodexo Remote Sites Scotland Ltd, Sodexo Global Services Ltd and Heritage Portfolio Ltd.

If you have any questions, comments, and requests regarding this privacy notice, you can email your local Data Protection contact, [DataProtection.UkandIE@Sodexo.com](mailto:DataProtection.UkandIE@Sodexo.com).

Sodexo is responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contracts to provide services. We may update this notice at any time but if we do so, we will update you on any changes as soon as reasonably practical.

You must read this notice, together with any related data protection policies and other privacy notices or updates we may issue from time to time so that you are aware of how and why we are using such information and what your rights are under data protection legislation.

## **2. DATA PROTECTION PRINCIPLES**

We will comply with data protection laws. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

## **3. THE KIND OF INFORMATION WE HOLD ABOUT YOU, HOW WE USE IT AND THE LAWFUL BASIS**

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We will only use your personal information when the law allows us to.

We collect and use information, such as identity and contact details, job performance, salary, and training, to perform the employment contract with staff, comply with legal requirements (such as PAYE) and our legitimate interests of running a business, health, and safety and providing services. Where we rely on legitimate interests, these are concerning expected business purposes, such as health and safety and are limited to respect our staff's privacy.

### **ANNEX A SETS OUT MORE DETAILS ABOUT THESE.**

Less commonly - we may also use your personal information in the following situations

1. Where we need to protect your vital interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.
3. Consent

Some of the above grounds for processing will overlap and there may be several grounds that justify our use of your personal information.

#### **4. HOW WE USE SPECIAL CATEGORY PERSONAL INFORMATION**

“Special categories” of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or trade union membership, require higher levels of protection. We also have in place an appropriate policy document for processing this type of Personal Data. Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing, and using this type of personal information. The usual reasons we process special categories of personal information are:

1. In limited circumstances, with your explicit written consent. Where we use biometric data for clocking in and out, this information can only be used with your consent. You will be offered an alternative to the collection of biometric data.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring, health, and safety or concerning our occupational pension scheme.

Less commonly, we may process this type of information where it is needed concerning legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Annex B sets out more details about these.

#### **5. INFORMATION ABOUT CRIMINAL CONVICTIONS, CONVICTIONS, OFFENCES, AND INVESTIGATIONS**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our Global Data Protection Policy and, where relevant, the Employment Checks Policy. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We only collect this information where it is appropriate given the nature of the role.

Less commonly, we may use information relating to criminal convictions where it is necessary for relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

#### **JUSTICE SERVICES**

Where your role means your work is concerning prisons some of your Personal Data will be used outside of the scope of GDPR and will fall under Law Enforcement Processing and biometric data may

be required for security reasons within a prison. You will be provided with further information about this if it applies to you.

## **6. HOW IS YOUR PERSONAL INFORMATION COLLECTED?**

We collect personal information about employees, workers, and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment business/agency or background check provider and may use public information on social media. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies, existing or potential clients or customers, suppliers, subcontractors, trade partners or external service providers.

We may also collect personal information from the trustees or managers of pension arrangements operated by a group company.

We will collect additional personal information in the course of job-related activities whilst you are working for us, this can include information from automated systems or third parties.

### **6.1 MONITORING**

There may be specific monitoring which takes place as part of your role, you will be provided with more information about this if it applies to you. For example, it may be necessary for your health and safety to know your location if you are working on your own in a remote place.

We may operate CCTV on some of our sites and if you are working on one of our client's sites, such as providing security services in a hospital, the client may operate CCTV or Body Worn cameras (BWC). CCTV/BWC is usually installed for the purposes of the detection or prevention of crime and public safety. It may also on occasion be used in disciplinary or other HR investigations.

If you use digital work equipment, there will be security scans, for example, to check for viruses.

## **7. AUTOMATED DECISION-MAKING**

Automated decision-making takes place when an electronic system uses personal information to make a decision about you, without human intervention. If automated decision making has legal or other significant effects, we are only allowed to use automated decision-making in the following circumstances:

1. With your consent and where appropriate measures are in place to safeguard your rights.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, if it is authorised in a law which sets out appropriate measures to safeguard your rights.

If we make an automated decision based on special category information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless we have a lawful basis for doing so and we have notified you.

## **8. IF YOU FAIL TO PROVIDE PERSONAL INFORMATION**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

## **9. CHANGE OF PURPOSE**

We will only use your personal information 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 we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **10. DATA SHARING**

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK/ EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

### **10.1. Why might you share my personal information with third parties**

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, to provide client services or where we have another legitimate interest in doing so.

We would expect to disclose relevant parts of your personal data where appropriate and necessary to the following classes of recipients:

1. internally to colleagues or managers as part of the employment relationship.
2. externally to regulatory or statutory bodies such as HMRC, or for the purposes of Pensions administration, benefits provision, participation in share plans, disclosures to the stock exchange, disclosure to shareholders such as directors' remuneration, auditors, employee engagement surveys, training providers and payroll.
3. externally to clients of Sodexo, where your role means you would be working on a client's premises or systems, when retendering a contract, or in the context of a possible sale or restructuring of the business.
4. To suppliers or partners in order to provide benefits, including to enable the supplier to verify that you are entitled to the benefit ( for example by evidencing that you are a Sodexo employee).
5. Under TUPE regulations or concerning a sale or acquisition of a business.
6. Other Group Companies, where it is required for providing joint services such as IT (including hosting and system maintenance support), Information security, HR, succession planning, business re-organisation, reporting (such as company performance), administering group pensions or share plans, legal claims, and legal obligations.

7. if the law or a legal procedure requires us to do so, (ii) in response to a request by public authorities or other officials or (iii) if we are of the opinion that transferring these data is necessary or appropriate to prevent any physical harm or financial loss or in respect of an investigation concerning a suspected or proven unlawful activity (iv) providing the service/contract, (v) fraud protection and credit risk reduction, (vi) to protect rights, property and safety or enforce our agreements, (vii) buy or sell business assets

If a request for disclosure is made from a third party, such as the police or an insurer, we decide whether to disclose information on a case-by-case basis.

We may also share your Personal data with authorized service providers, called data processors (for example: technical service providers), that we may call upon for the purpose of providing our Services. We ensure that every disclosure of your Personal data to an authorized service provider is framed by a data processing agreement, reflecting the commitments laid out in this policy. We do not authorize our service providers to use or disclose your data, except to the extent necessary to deliver the Services on our behalf or to comply with legal obligations.

## **10.2. Third-party service providers**

Our third-party service providers (data processors) are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and following our instructions.

## **10.3. Transferring information outside the UK**

As SODEXO is an international group, your Personal data may be transmitted to internal or external recipients that are authorized to perform Services on our behalf. Data protection law does not allow the transfer of Personal Data to third countries outside UK and EEA that do not ensure an adequate level of data protection. Some of the third countries in which Sodexo operates outside UK and EEA do not provide the same level of data protection as the country in which you reside and are not recognized by the European Commission or ICO as providing an adequate level of protection for individuals' data privacy rights.

We have also implemented appropriate safeguards to ensure an adequate level of protection of your Personal data, even if the Personal data is processed by another Sodexo entity that did not collect your Personal data originally.

Sodexo has implemented the Sodexo's Binding Corporate Rules (BCRs) within Sodexo Group. Therefore, even if the third countries in which Sodexo entities operate are located outside of the European Economic Area, your Personal data is protected in the same way that they would have been by any entity located within the European Economic Area.

To guarantee the security and confidentiality of Personal data thus transmitted, we will take all necessary measures to ensure that this data receives adequate protection, such as entering into data transfer agreements with the recipients of your personal data based on the applicable standard contractual clauses ("SCCs") or IDTA other valid transfer mechanisms and we carry out, in accordance with the European Court of Justice's decision of 16 July 2020 "Schrems II" (Case C 311-18), a risk

assessment of the transferred data. If you would like to receive a copy of the safeguards in place to secure data transfers outside the UK or European Economic Area, please contact the Data Protection Officer.

## **11. DATA SECURITY**

We implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful alteration or loss, or from unauthorized, use, disclosure, or access, in accordance with our Group Information and Systems Security Policy.

We take, when appropriate, all reasonable measures based on Privacy by design and Privacy by default principles to implement the necessary safeguards and protect the Processing of Personal Data. We also carry out, depending on the level of risk raised by the processing, a Privacy impact assessment (“PIA”) to adopt appropriate safeguards and ensure the protection of the Personal Data. We also provide additional security safeguards for data considered to be Sensitive Personal Data. Where We have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential.

Unfortunately, the transmission of information via the internet is not completely secure. Although We will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once We have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

## **12. STORAGE LIMITATION AND ACCURACY**

Sodexo will keep Personal Data that is processed accurate and, where necessary, up to date. We will store your Personal data only for as long as necessary to fulfil the purposes for which it was collected and processed. This period may be extended, if applicable, for any amount of time prescribed by any legal or regulatory provisions that may apply.

To determine the retention period of your Personal data, we take into consideration several criteria such as:

- The purpose for which we hold your Personal data (e.g., the employment relationship)
- Our legal and regulatory obligations in relation to that Personal data (e.g., accounting reporting obligations).
- Any specific requests from you in relation to the deletion of your Personal data or Account.
- Any statutory limitation periods allowing us to manage our own rights, for example the defence of any legal claims in case of litigation; and
- Any local regulations or guidance (e.g., regarding cookies).
- 

Please find more information about the storage period of your Personal data in Annex 1 below.

## **13. RIGHTS OF ACCESS, CORRECTION, ERASURE AND RESTRICTION**

### **13.1. Your duty to inform us of any changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.



## 13.2. Your Rights

Sodexo is committed to ensure protection of your rights under applicable laws. You will find below a table summarizing your different rights:

<b>Right of access And Rectification</b>	<p>You can request access to your personal data. You may also request rectification of inaccurate personal data, or to have incomplete personal data completed.</p> <p>You can request any available information as to the source of the personal data and you may also request a copy of your personal data being processed by Sodexo.</p>
<b>Right to be forgotten</b>	<p>Your right to be forgotten entitles you to request the erasure of your personal</p> <ol style="list-style-type: none"><li>i. data in cases where: the data is no longer necessary</li><li>ii. you choose to withdraw your consent</li><li>iii. you object to the processing of your personal data by automated means using technical specifications</li><li>iv. your personal data has been unlawfully processed</li><li>v. there is a legal obligation to erase your personal data</li><li>vi. erasure is required to ensure compliance with applicable laws</li></ol>
<b>Right to restriction of processing</b>	<p>You may request that processing of your personal data be restricted</p> <ol style="list-style-type: none"><li>i. in the cases where: you contest the accuracy of the personal data</li><li>ii. Sodexo no longer needs the personal data, for the purposes of the processing</li><li>iii. you have objected to processing for legitimate reasons</li></ol>



**Right to data portability**

You can request, where applicable, the portability of your personal data that you have provided to Sodexo, in a structured, commonly used, and machine-readable format and you have the right to transmit this data to

- a) another Controller without hindrance from Sodexo where:  
the processing of your personal data is based on consent or on a
- b) contract: and  
the processing is carried out by automated means.

You can also request that your personal data be transmitted to a third party of your choice (where technically feasible).

**Right to object to processing including direct marketing**

You can object to us using your Personal Data for direct marketing. You can also contact us to object to how we are using your Personal Data for any other reason, but we may not have to stop using it for this purpose.

**Right to Withdraw Consent**

If We process your personal data since your consent, you can withdraw your consent at any time.

**Right not to be subject to automated decisions**

You have the right not to be subject to a decision based solely on automated processing, including profiling, which has a legal affect upon you or significantly affects you. You have the right to object to processing including direct marketing which uses profiling.

## Right to lodge a complaint

Within the EU, you can choose to lodge a Complaint with the Data Protection Supervisory Authority in the country of your habitual residence, place of work or place of the alleged infringement, regardless of whether you have suffered damages.

You have also the right to lodge your Complaint before the courts where the Sodexo entity has an establishment or where you have your habitual residence. In the UK you have the right to lodge a complaint with the Information Commissioner or lodge a Complaint before the courts.

[You can use this form to make a request.](#) This electronic system allows you to log in and see the progress of your request, see and send messages and review your documents securely. This system is called One Trust and after making the request you will be sent details about how to log on.

Alternatively, you can also send your request by email to [DSAR.UKandIE@sodexo.com](mailto:DSAR.UKandIE@sodexo.com), in writing to 310 Broadway, Salford, M50 2UE or by calling Sodexo People Centre on 0845 603 3644 and asking for DSAR team. The team will liaise with you about how you to contact you about your request and receive information. Please note that it is usually necessary to arrange a telephone appointment to discuss your request once it has been made. You can also contact the DPO at this address or by email to [DataProtection.UKandIE@sodexo.com](mailto:DataProtection.UKandIE@sodexo.com) .

If you wish to unsubscribe to marketing emails communications, you can also do so by using the unsubscribe function on the email.

For more details, please consult the Global Data Protection Rights Management Policy.

### Third Party beneficiary rights

If applicable in your country, you can enforce the third-party beneficiary rights afforded to you by the Sodexo BCRs.

### 13.3. No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

### 13.4. What we may need from you

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.

### **13.5 Right to Withdraw Consent**

In the limited circumstances where you may have provided your specific consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. When you provide your consent, you will ordinarily be provided with the method to withdraw it. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## **14. CHANGES TO THIS PRIVACY NOTICE**

We reserve the right to amend this privacy notice at any time and will notify you of any changes as soon as reasonably practicable. We may also notify you in other ways, from time to time, about any changes we may make to the processing of your personal data.

### **LINKS AND SOCIAL**

Links to other websites should not be considered as navigation tracking and we decline any responsibility concerning the personal data protection practices implemented by these third-party companies, each of which acts as a separate Controller of your Personal data on their own perimeter. Once you leave our Site or click on the logo/link to one of these social networks, it is your responsibility to check the privacy policy applicable to that other platform.

When you click on social media icons, we may have access to the personal data that you have made public and accessible via your profiles on the social networks in question. If you do not want us to have access to your Personal data published in the public spaces of your profile or your social accounts, then you should use the procedures provided by the social networks in question to limit access to this information.

Our legitimate interests are to run a business, provide and improve our services to clients, retain and develop staff, health, and safety, keep our data, premises and equipment secure, marketing and PR and corporate social responsibility.

## Annex A

### INFORMATION ABOUT THE PROCESSING OF YOUR PERSONAL DATA

Purpose of the Processing	Personal data collected	Legal basis of the Processing	Retention of the Personal data
Providing salary, benefits, and pensions, share plans, bonuses, administering absence leave and sick pay and if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance Contributions (NICs).	Identity data Contact data Financial data Transaction data Technical data Profile data	Performance of a contract to which the data subject is party (or steps to enter the contract)  Consent  Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements (e.g., pensions)
Checking you are legally entitled to work in the UK/ROI and checking your identity	Identity data Contact data	Legal Obligation  Performance of a contract to which the data subject is party (or steps to enter the contract)	This information is retained three years after the end of the contractual relationship
Maintaining and processing general and personal records necessary to manage the employment relationship and operate the contract of employment	Identity data Contact data Financial data Transaction data Technical data Profile data	Performance of a contract to which the data subject is party Legitimate Interest Legal Obligation	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and

			until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements
Allocating duties and responsibilities and managing those duties and the business activities to which they relate and information from job activities.	Identity data Contact data Financial data Transaction data Technical data Profile data	Performance of a contract to which the data subject is party Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements
Carrying out formal and informal appraisals or reviews and personal development.  Managing conduct, performance, and absence; and employee evaluations.	Identity data Contact data Transaction data Technical data Profile data	Performance of a contract to which the data subject is party Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements
Managing and investigating grievances and disciplinary action.	Identity data Contact data Financial data Transaction data Technical data Profile data	Performance of a contract to which the data subject is party Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements
Monitoring (CCTV, BWC),	Identity data Contact data Transaction data Technical data Profile data	Legitimate Interest Legal Obligation	Information retained on CCTV or similar is not usually kept longer than 28 days. It may be retained for longer in the event of an incident. In the event of an incident or reported incident, we may seek permission from our client to review and use CCTV and BWC footage of the incident in HR investigations and legal

			proceedings and where appropriate review further footage for other potential incidents.
Portoring	Identity data Contact data Financial data Transaction data Technical data Profile data Location data	Performance of a contract to which the data subject is party Legitimate Interest	Information is anonymised after 12 months
Clocking in and out	Identity data Contact data Transaction data Technical data Profile data Location data	Performance of a contract to which the data subject is party Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements
Development requirements, providing, monitoring and maintaining training, skills for use internally and where appropriate supplying that information to customers and relevant third parties.	Identity data Contact data Financial data Transaction data Technical data Profile data	Performance of a contract to which the data subject is party Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements
making a decision about your recruitment or appointment. salary reviews and compensation.  Assessing qualifications for a particular job or task, including decisions about promotions.	Identity data Contact data Financial data Transaction data Technical data Profile data	Performance of a contract to which the data subject is party Legitimate Interest Legal Obligation	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements

<p>Determining the terms on which you work for us.</p> <p>Making decisions about your continued employment or engagement.</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Performance of a contract to which the data subject is party Legitimate Interest</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Making arrangements for the termination of our working relationship.</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Performance of a contract to which the data subject is party Legitimate Interest</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Dealing with legal disputes involving you, or other employees, workers and contractors, clients including accidents at work.</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Performance of a contract to which the data subject is party Legitimate Interest Legal Obligation</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Ascertaining your fitness to work. Managing sickness absence.</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Performance of a contract to which the data subject is party Legitimate Interest Consent Legal Obligation</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Complying with health and safety obligations, including carrying night staff and lone worker checks, and investigating LTIs</p>	<p>Identity data Contact data Financial data Transaction data</p>	<p>Performance of a contract to which the data subject is party</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual</p>



	Technical data Profile data	Legitimate Interest Legal Obligation Consent	relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements. Some health and safety requirement have a longer period, e.g., COSHH.
Employee elections and employee representative meetings.	Identity data Contact data Transaction data	Performance of a contract to which the data subject is party Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements
To conduct data analytics studies to review and better understand employee retention and attrition rates. Employee engagement.	Identity data Contact data Financial data Transaction data Technical data Profile data Location data	Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements. Information obtained for equalities monitoring should be anonymised 2 years after the contract ends.
Succession planning, Improving staff retention, health and safety	Identity data Contact data Financial data Transaction data Technical data Profile data Health Data	Legitimate Interest	The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements

<p>operating and improving and extending our services to clients and service users and business</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Legitimate Interest</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Acquisitions/mergers and sale of businesses including TUPE</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Legitimate Interest Legal Obligation Performance of a contract to which the data subject is party</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Business management and planning, including accounting and auditing, running and improving our business, business development, recovering payments, keeping accounting records, security, health and safety, fraud prevention customer service, statistical analysis and marketing including segmenting, bids, acquiring and disposing of businesses, governance.</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Legitimate Interest Legal Obligation Performance of a contract to which the data subject is party</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Manage and monitor our relationships with existing and potential customers and clients. Carry out the service provided by us or a client of ours/previous provider- steps to enter contract or perform/fulfil the contract.</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Legitimate Interest</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>

<p>To prevent fraud and monitor compliance with our policies and legal requirements, such as data protection, anti-bribery and corruption and Speak Up.</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data Location data</p>	<p>Legitimate Interest Legal Obligation</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Disclosure of basic personal data and contact information to third party contacts including customers, suppliers and other associates of Sodexo necessary in order to operate the relationship with those third parties and ensuring the smooth conduct of the business. Administering the contracts, we have with our third-party clients to provide Quality of Life Services</p>	<p>Identity data Contact data Financial data Transaction data Technical data Profile data</p>	<p>Legitimate Interest</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>
<p>Where reasonably necessary for publicity material or obtaining business including annual reports or similar business documentation and tenders for work.</p>	<p>Identity data Contact data Transaction data</p>	<p>Legitimate Interest</p>	<p>The usual limitation period in civil and commercial matters is six (6) years. We will keep the personal data for up to 7 years after the end of the contractual relationship. In the event of a dispute, this data is kept for the duration of the procedure and until the expiration of ordinary and extraordinary remedies. Unless it is required for longer for legal obligations or accounting requirements</p>

<p>Information collected through websites and other channels relating to use age for recruitment, training, providing information about benefits and internal engagement</p>	<p>Identity data  Contact data  Financial data  Transaction data  Technical data  Profile data</p>	<p>Legitimate Interest  Legal Obligation  Performance of a contract to which the data subject is party</p>	<p>We will keep your data for a period of three (3) years after the end of the competition or the last contact you initiated.</p>
--	--	--	---

**Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender, images

**Contact Data** includes address, email address and telephone numbers.

Date of Birth, National Insurance number, next of kin, emergency contact information, gender, dependants, gender, identity information and right to work information Results of HMRC employment status check details of your interest in and connection with the intermediary through which your services are supplied

Passport/driving licence, identity info, (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).

**Financial Data** includes bank details and payment card details, payments made.

**Transaction Data** salary benefits, pension information, start and end date of employment, reasons for leaving, contract details, work location and photographs. payroll records and tax status information, work location

Recruitment information training records, attendance records, information about activities undertaken as part of the working relationship including performance and absences.

Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).

Compensation history.

Performance information including appraisals, performance reviews, ratings, training that you have participated in, performance improvement notices or warnings and any associated correspondence.

Disciplinary and grievance information including any warnings issued to you and related correspondence

**Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access our website. CCTV footage and other information obtained through electronic means such as swipe card records.

**Profile Data** includes your username and password, purchases or orders made by you, your interests, preferences, feedback, and survey responses.

**Usage Data** includes information about how you use our website, products, and services. Information about your use of our information and communications systems. Company email systems. Staff surveys and feedback

**Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

**Annex B**

**Special Category Personal Data**

<p>Information about your health, including any medical condition, health and sickness records, accidents at work and including keeping records of decisions and actions.</p>	<p>Assess eligibility for sick pay or other insurance, health or pension or statutory/contractual benefits.</p> <p>To monitor and manage sickness and other absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions, and permanent health insurance.</p> <p>To determine fitness for work generally or at a particular time or for particular roles or duties, making decisions regarding alternative duties, alternative roles or adjustments to those roles or duties, to assist in achieving a return to work, making decisions about employment and continued employment and appeals and otherwise in accordance with any absence procedure operated by Sodexo.</p> <p>Health and safety in the workplace. (and to the public, clients and users of our services) , including investigation of work place injuries, occupational health reports, lone worker and night staff checks.</p> <p>Where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision.</p> <p>Where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.</p>
---	--

	<p>If you apply for an ill-health pension under a pension arrangement operated by a group company, we will use information about your physical or mental health in reaching a decision about your entitlement.</p>
<p>Information about your race or national or ethnic origin, disability, age, religious, philosophical beliefs, and sexual orientation/gender assignment, or your sexual life or sexual orientation.</p>	<p>Where it is collected for monitoring promoting and reporting on and taking actions in respect of equal opportunities and diversity.</p> <p>Or for an employment purpose, such as information about disabilities to make reasonable adjustments or nationality for checking right to work.</p>
<p>Trade union membership.</p>	<p>We will use trade union membership information to pay trade union premiums, register the status of a protected employee and comply with employment law obligations.</p>
<p>Biometric Data</p>	<p>Where this is used as part of a time and attendance system. This is on the basis of consent and alternatives are offered.</p>