

Group Colleague Privacy Notice

1. What does this document cover?

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, including the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR). It applies to all employees, workers and contractors. Individuals who normally reside in Kenya are referred to the information that is contained in the addendum at pages 15 – 19.

The Controller of your personal information is the IPL Group company that employs or engages you. Details for all group companies are set out below:

- International Procurement and Logistics Limited whose head office is 1 Foxbridge Way, Normanton, England, WF6 1TN;
- International Procurement and Logistics (Spain) S.L. of Calle Venecia 1, 1 izq, 30700, Torre Pacheco, Murcia, Spain;
- Forza Foods Limited of 62 Devilliers Way, Normanton, England, WF6 1GX; and,
- Kober Limited of 4 Hanging Wood Way, Cleckheaton, England, BD19 4TS.

2. What is personal information?

Personal Information (also known as personal data) is any information that identifies someone and any information that relates to that identified person. For example, your name and national insurance number are information that identifies you, and your working hours relate to you.

Some information is classed as "special category" under data protection law. This particularly sensitive personal information (such as information about health, racial or ethnic origin) requires higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information.

3. Our commitment to data protection

We will comply with data protection law and ensure that the personal information we hold about you will be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about; and,
- retained securely.

4. What personal information do we hold?

We do not process more information than we need.

The descriptions below summarise the information we hold.

Description	Examples of the type of data involved
Identity data	<ul style="list-style-type: none">• First and last name• Preferred title• Date of birth• Gender• Username• Marital status• National Insurance number• Passport Number• Biometric Identifiers (such as fingerprint and facial representations)
Contact data	<ul style="list-style-type: none">• Address• Email address• Telephone number• Details for any additional persons for whom contact details are required, such as next of kin and emergency contact details
Image data	<ul style="list-style-type: none">• CCTV video and photographic images• IPL Group videos and images created for internal and external promotional/business purposes• Biometric Identifiers (such as fingerprint and facial representations)
Financial and transaction data	<ul style="list-style-type: none">• Bank account details• Payroll records• Tax status• Salary• Pension information
Technical data	<ul style="list-style-type: none">• Data from the access / entrance controls at our sites• Internet protocol address• Login data• Browser type and version• Time zone setting• Geolocation data• Data about the use of our IT systems, network and email service• Data about employee use of laptops and phones• Data obtained from cookies, web logs and other similar technologies• Browsing and search history• Internet browsing data• Data contained in emails stored in our systems
Usage data	<ul style="list-style-type: none">• File and folder creations, deletions and access• Blocking of emails that contain 'danger words', obscene language etc.

Employee benefits data	<ul style="list-style-type: none"> • Your personal information for your company life insurance cover • Your personal information for your company private health cover • Your personal information for your company pension • Name, address and other personal information for any beneficiaries under your company life insurance, private health care and company pension
Recruitment data	<ul style="list-style-type: none"> • Right to work evidence, such as copies of passports and / or birth certificates • Information we collect from third parties, including former employers • Results of anti-corruption and other background checks • References • Information included in an application form, CV or covering letter
Legal and compliance data	<ul style="list-style-type: none"> • Results of HMRC employment status checks • Details of your interest in and connection with the intermediary through which your services are supplied • Contracts of employment and any amendments to them • Training records and professional memberships
HR data	<ul style="list-style-type: none"> • Start date and, if different, the date of continuous employment • Location of employment or workplace • Job titles • Work history • Working hours • Forms and other records of holiday, sickness, maternity, paternity and adoption leave • Compensation history • Performance information • Appraisals / performance reviews • Disciplinary, grievance and any other employment matters • Where relevant, social media activity • Leaving date and reason for leaving
Time and attendance data	<ul style="list-style-type: none"> • Records from employee clocking in systems
Incident data	<ul style="list-style-type: none"> • Information about accidents and 'near misses' • Statements from witnesses • Where relevant, social media
Employee productivity data	<ul style="list-style-type: none"> • Records from employees usage and interaction with, including but not limited to, Redzone, Marco and Lineview productivity software platforms

5. What special category personal information do we hold?

We collect, store and use the following more sensitive types of personal information.

Description	Examples of the type of data involved
Equal opportunities monitoring data	<ul style="list-style-type: none">Information about sex, sexual orientation, race, ethnicity and similar equal opportunity data
Health data	<ul style="list-style-type: none">Information about health, including any medical conditionSickness records and similarMedical certificates and similarGP correspondence and similarGP and occupational health reportsInformation about accidents and 'near misses'Drug, alcohol and coronavirus test results
Criminal convictions	<ul style="list-style-type: none">Information about unspent criminal convictions and offences
Biometric data	<ul style="list-style-type: none">Biometric Identifiers (such as fingerprint and facial representations) used for secure log in to devices (where consent is given), such as MS Hello.

6. Where do we get our information?

- Directly from you when you provide it to us yourself or an employment agency acting for you does.
- From former employers and background check agencies.
- From third parties, such as the government tax authority (HMRC) and our company pension provider.
- We will collect information in the course of job related activities when you are working for us, including about your use of our IT equipment and internet connectivity.

7. How will we use information about you?

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

Most commonly, we will use your personal information in the following circumstances:

- where we need to perform the contract we have entered into with you;
- where your explicit consent has been given;
- where we need to comply with a legal obligation; and,
- when it is necessary for legitimate interests pursued by us or a third party, and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- where we need to protect your interests (or someone else's interests); and,
- when necessary, in the public interest.

Situations in which we will use your personal information

The situations in which we will use your personal information and the categories of data involved are set out below. In the table, we have also indicated the lawful basis for which we are processing or will process your personal information. Where a legitimate interest is involved, we state what the legitimate interest is.

Purpose / situation	Examples of data involved	Our lawful basis for processing
Checking you are legally entitled to work in relevant countries, and other similar purposes	<ul style="list-style-type: none"> Right to work evidence, such as copies of passports and / or birth certificates 	<ul style="list-style-type: none"> Legal obligation (Article 6(1)(c) of the GDPR)
Making a decision about your recruitment or appointment, and other compatible purposes	<ul style="list-style-type: none"> References Information included in an application form, CV or covering letter Notes taken at interviews Training records Professional memberships 	<ul style="list-style-type: none"> Processing at your request, before entering a contract (Article 6(1)(b) of the GDPR)
Assessing qualifications for a particular job or task, including decisions about promotions, as well as other similar purposes	<ul style="list-style-type: none"> As above Performance information 	<ul style="list-style-type: none"> Processing at your request, before entering a contract (Article 6(1)(b) of the GDPR)
Determining the terms on which you work for us, and other compatible purposes	<ul style="list-style-type: none"> Contracts of employment and any amendments to them Employment history (including job titles, work history, working hours, holidays) Compensation history IR35 assessment 	<ul style="list-style-type: none"> Legal obligation (Article 6(1)(c) of the GDPR)
Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions, and other compatible purposes	<ul style="list-style-type: none"> First and last name National Insurance number Address Bank account details Payroll records Tax status Salary Annual leave Pension details Attachment of earnings deductions e.g. child support Employee benefits information 	<ul style="list-style-type: none"> Legal obligation (Article 6(1)(c) of the GDPR)
Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties and liaising with your pension provider and any other provider of employee benefits, and other compatible purposes	<ul style="list-style-type: none"> First and last name Date of birth Gender National Insurance number Details of any additional persons for whom contact details are required, such as your nominated beneficiaries 	<ul style="list-style-type: none"> Legal obligation (Article 6(1)(c) of the GDPR)

To manage attendance and timekeeping, and similar purposes	<ul style="list-style-type: none"> • System records for the devices colleagues use to clock in and out of work 	<ul style="list-style-type: none"> • Legal obligation (Article 6(1)(c) of the GDPR)
Business management and planning, including accounting and auditing and compatible purposes (Including IPL Group overseas legal compliance requirements)	<ul style="list-style-type: none"> • Payroll records • Tax status • Salary • Other payments • Passport and/or Identity documents 	<ul style="list-style-type: none"> • Legal obligation (Article 6(1)(c) of the GDPR)
Conducting performance reviews, managing performance and determining performance requirements and similar purposes	<ul style="list-style-type: none"> • Appraisal / performance review forms • Feedback • Where relevant, information relating to absences, training records, disciplinary, grievances and any other employment matters 	<ul style="list-style-type: none"> • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Making decisions about salary reviews, remuneration and similar purposes	<ul style="list-style-type: none"> • Salary information • Salary history • Appraisal / performance reviews • Feedback 	<ul style="list-style-type: none"> • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Ensuring a safe and secure environment, to prevent and detect crime, disciplinary proceedings and to investigate accidents and incidents, and other similar purposes	<ul style="list-style-type: none"> • CCTV footage • Images from CCTV • Accident information • 'Near miss' information • Drug and alcohol testing 	<ul style="list-style-type: none"> • Processing necessary to perform a contract (Article 6(1)(b) of the GDPR) • Legal obligation (Article 6(1)(c) of the GDPR) • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Gathering evidence for possible grievance or disciplinary hearings and other compatible purposes	<ul style="list-style-type: none"> • Where relevant, statements from witnesses, social media, information relating to absences, training, disciplinary matters, grievances and any other employment matters, photographs and video from CCTV, data on computer network and email use (including data obtained from cookies, web logs and other similar technologies), time and attendance data, alcohol and drugs testing data, and accident and incident data 	<ul style="list-style-type: none"> • Processing necessary to perform a contract (Article 6(1)(b) of the GDPR) • Legal obligation (Article 6(1)(c) of the GDPR) • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)

Making decisions about your continued employment or engagement and compatible purposes	<ul style="list-style-type: none"> • Probation, appraisal and performance review forms • Feedback • Where relevant, evidence gathered in relation to grievance, disciplinary or any other employment matters 	<ul style="list-style-type: none"> • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Making arrangements for the termination of our working relationship, and other compatible purposes	<ul style="list-style-type: none"> • Contracts of employment and any amendments to them • Start date and, if different, the date of your continuous employment • Employment records • Appraisal / performance review forms • Where relevant, records and evidence gathered in relation to any employment matters 	<ul style="list-style-type: none"> • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Education, training and development requirements, and other similar purposes	<ul style="list-style-type: none"> • Recruitment records • Training records • Where relevant, records and evidence gathered in relation to grievance, disciplinary and any other employment matters, appraisal and / or performance review forms, feedback etc. • Monitoring data obtained from (including but not limited to) Redzone, Marco and Lineview systems. 	<ul style="list-style-type: none"> • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Dealing with legal issues and situations involving you, or other employees, workers and contractors, including accidents at work	<ul style="list-style-type: none"> • Where relevant, statements from witnesses, social media, information relating to absences, training, disciplinary matters, grievances and any other employment matters, photographs and video from CCTV, data on computer network and email use (including data obtained from cookies, web logs and other similar technologies), time and attendance data, alcohol and drugs testing data, and accident and incident data 	<ul style="list-style-type: none"> • Legal obligation (for UK and EU, Article 6(1)(c) of the GDPR) • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Complying with health and safety and associated obligations	<ul style="list-style-type: none"> • Information about accidents and 'near misses' to allow us to investigate the causes and prevent reoccurrence 	<ul style="list-style-type: none"> • Legal obligation (Article 6(1)(c) of the GDPR) • Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)

Monitoring use of IT systems, internal portals, network and equipment to ensure compliance with our IT policies, and other compatible purposes	<ul style="list-style-type: none"> Information about how you use our computer network, internal portals and email service, as well as work equipment such as laptops and mobile phones (including the data obtained from cookies, web logs and other similar technologies) 	<ul style="list-style-type: none"> Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Information security, including preventing unauthorised access to our computers, systems and network, and to prevent malicious software distribution, and other compatible purposes	<ul style="list-style-type: none"> Information about how you use our computer network and email service, as well as work equipment such as laptops and mobile phones (including the data obtained from cookies, web logs and other similar technologies) 	<ul style="list-style-type: none"> Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Data analytics studies to review and better understand employee retention and attrition rates, and other compatible purposes	<ul style="list-style-type: none"> Leaving date Reason for leaving 	<ul style="list-style-type: none"> Legitimate interest in running our business and managing you (Article 6(1)(f) of the GDPR)
Business continuity purposes following the cessation of your employment for any reason, including to allow us to ensure that any emails received by you are responded to and any projects you have been involved in can continue to progress	<ul style="list-style-type: none"> Leaving date Information about how you use our computer network and email service, as well as work equipment such as laptops and mobile phones (including the data obtained from cookies, web logs and other similar technologies) The contents of emails addressed to you The contents of documents contributed to by you 	<ul style="list-style-type: none"> Legitimate interest of running our business well (Article 6(1)(f) of the GDPR)
Any content featuring employees produced for use on our website or social media (including but not limited to Facebook, X (formally Twitter)) such as videos, authored articles, blog posts and speech transcripts.	<ul style="list-style-type: none"> First and last name Featured images Featured videos Authored testimonies 	<ul style="list-style-type: none"> Consent has been obtained (Article 6(1)(a) of the GDPR)

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 it for an unrelated purpose, 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 where required or permitted by law.

8. How do we use particularly sensitive personal information?

We may process special categories of personal information, such as information about your health, biometric identifies, racial or ethnic origin in the following circumstances:

1. in limited circumstances, with your explicit consent;
2. where we need to do so in order to perform our legal obligations;
3. where it is needed in the public interest, such as for equal opportunities monitoring; and,
4. where it is necessary to protect you or another person from harm.

Less commonly, we may process information like this in relation to legal claims, or to protect your interests (or someone else's interests) and you are not capable of giving consent, or have already made the information public.

Situations in which we will use your sensitive personal information

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as when it is in the public interest to do so, or where we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

The lawful basis we rely on to process any sensitive personal information is article 9(2)(b) of the GDPR, which relates to our obligations in employment and the safeguarding of your fundamental rights, and Schedule 1 part 1(1) of the DPA 2018 which again relates to processing for employment purposes. Examples of the situations where we process this data are:

Purpose / situation	Examples of data involved
<ul style="list-style-type: none">• To ensure your health and safety in the workplace, to provide appropriate workplace adjustments and similar purposes	<ul style="list-style-type: none">• Information about your physical or mental health, or disability status• Medical certificates• Doctor and other medical practitioner correspondence• GP and occupational health reports
<ul style="list-style-type: none">• Assessing your fitness to work, to monitor and manage sickness absence and other similar situations	<ul style="list-style-type: none">• Information about your physical or mental health, or disability status• Records of sickness and other absences• Medical certificates, GP and occupational health reports and correspondence
<ul style="list-style-type: none">• To administer statutory maternity pay, statutory sick pay, your pension and health insurance, and similar situations	<ul style="list-style-type: none">• Information about your physical or mental health, or disability status• Records of sickness and other absences• Medical certificates, GP and occupational health reports and correspondence
<ul style="list-style-type: none">• Administering payments to trade unions from salaries of colleagues who are trade union members	<ul style="list-style-type: none">• Employee mandates for payments to trade unions and associated cancellation forms

<ul style="list-style-type: none"> If you wish to join any eligible company life insurance policy or similar, we will process information about your health 	<ul style="list-style-type: none"> Information about your physical or mental health, or disability status Records of sickness and other absences Medical certificates, GP and occupational health reports and correspondence
<ul style="list-style-type: none"> Health and safety obligations 	<ul style="list-style-type: none"> Information about accidents and 'near misses' to allow us to investigate the causes and prevent reoccurrence
<ul style="list-style-type: none"> If we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental or emotional harm or to protect physical, mental or emotional well-being 	<ul style="list-style-type: none"> Information about your physical or mental health, or disability status
<ul style="list-style-type: none"> Equal opportunities monitoring 	<ul style="list-style-type: none"> Information about your ethnic group and nationality to ensure meaningful monitoring and reporting

In rare and limited circumstances, we may approach you for your written consent to allow us to process other sensitive data, article 9(2)(a) of the GDPR. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us. Examples of when we process sensitive personal information in this way are:

Purpose / situation	Examples of data involved
<ul style="list-style-type: none"> Microsoft Hello - secure laptop and mobile log in 	<ul style="list-style-type: none"> Biometric identifies fingerprint and facial information

Information about criminal convictions

Where appropriate, we will collect information about criminal convictions as part of the recruitment process, when you notify us and when such information otherwise emerges. We are able to use your personal information in this way for our legitimate business purposes.

9. Do we share your information with anyone?

We may have to share your data with third parties, including service providers and other entities in the IPL Group. We will require these parties to ensure the security of your data and to treat it in accordance with the law.

When might we share personal information with other entities in the group?

We will share personal information with other entities in our IPL Group as part of our regular reporting activities on company performance, in the context of a business reorganisation or IPL Group restructuring exercise, for system maintenance support and hosting of data, and for similar or compatible purposes*.

We may also share your special category data with other entities within the IPL Group including the IPL Group occupational health provider. If we do so, we will provide you with full details of the information that we are sharing and the reason why it is being shared.

Which third-party service providers process personal information?

"Third parties" includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers:

- payroll services (applicable only to Forza and Kober colleagues and some non-UK based IPL colleagues);
- occupational health services (including the IPL Group occupational health provider), including assessments;
- training providers;
- corporate design/presentation providers;
- professional photographers;
- pensions administration*;
- benefits provision and administration*;
- legal and financial advice*;
- insurance services*; and,
- IT services.

** Including IPL Group overseas compliance requirements.*

Why might we share personal information with other third parties?

We will share your personal information with third parties when required by law, where necessary to administer our contract with you, and when we have a legitimate interest in doing so. In any scenario, we will satisfy ourselves that we have a lawful basis on which to share the information and document our decision-making.

For example:

- we may need to share your personal information with a regulator or, to otherwise comply with the law*. This may include making returns to HMRC and disclosures to shareholders such as directors' remuneration reporting requirements;
- we will disclose appropriate information (including CCTV footage) to law firms and insurance providers to obtain advice and as evidence in legal claims;
- we have legal obligations to share certain information with the Health and Safety Executive;
- we will share information with pensions and health insurance providers in relation to the administration of your policies and / or in relation to claims made*;
- if you are referred to our occupational health provider (including the internal IPL Group occupational health provider), we will share appropriate personal information with them so that they have the information they need to assess your health and welfare;
- we share information with our insurers that is relevant for them in processing an insurance claim*;
- we share information with our professional advisors, such as legal advisors, auditors, accountants, if disclosure is required for the professional advisor to provide advice or services to us*;
- we may share personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation, as far as possible, we will share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction*;
- we may share your information with external providers of training or when designs are created for external conferences and presentations. Once this transaction is completed this data will not be retained by the third party; and
- where consent has also been obtained, professional photographs which have been taken at corporate events. Once the transaction is completed this data will not be retained by the third party

** Including IPL Group overseas compliance requirements.*

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies and data protection law. 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 in accordance with our instructions.

10. How do we protect your personal information?

We have put in place appropriate policies, procedures and security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Details of these measures may be obtained from the IPL Legal and Compliance Team.

In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Where third parties process personal information out of the European Economic Area, we will always ensure that we have appropriate contractual protections in place to ensure a similar degree of protection in respect of your personal information.

We have procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

11. How long do we keep information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available to you:

IPL: On the Mitrefinch system, or by emailing the IPL Legal and Compliance team at Dataprotection@ipl-ltd.com

Forza / Kober: On the SharePoint Privacy Hub, or by emailing the IPL Legal and Compliance team at Dataprotection@ipl-ltd.com

To determine the appropriate retention period for personal data, we consider any applicable legal requirements, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure, the purposes for which we process the data and whether we can achieve those purposes through other means.

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, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

12. Your data protection rights

In relation to your personal information, you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. There are however some exemptions, which means that you may not always receive all the information we process.
- **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). There are some exemptions, which means we may not be able to delete all personal information we hold about you.
- **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 which makes you want to object to processing on this ground.
- **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. This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another, or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated.
- **Withdraw consent** where consent is the legal basis for processing your personal information. This means we will stop using this information and delete / destroy it.

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 clearly unfounded or excessive.

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. Exercising your rights, contacts and complaints

If you have any questions about this privacy policy or wish to exercise any of your rights, please get in touch with the IPL Legal and Compliance team by e-mailing Dataprotection@ipl-ltd.com

If you have any concerns about the way we process your personal data or are not happy with the way we have handled a request by you in relation to your rights, you also have the right to make a complaint to the Information Commissioner's Office. Their address is:

By Post:	First Contact Team Information Commissioner's Office Wycliffe House Water Lane Wilmslow SK9 5AF
----------	--

14. Data Protection Officer

We have appointed a Data Protection Officer to provide independent expert advice and monitor compliance with data protection laws. You can contact our Data Protection Officer in the following ways. Please mark your correspondence 'Data Protection Officer'.

By Email:	Dataprotection@asda.uk
By Post:	Data Protection Officer Compliance Team Asda House Great Wilson Street Leeds LS11 5AD

Addendum for Kenya

In addition to the information shared in the privacy notice, colleagues who normally reside in Kenya may have certain rights under the Kenyan Data Protection Act, 2019 (**KDPA**) and the Kenyan Data Protection (General Regulations) 2021 and local laws, regulations or guidelines implementing or supplementing KDPA.

Other personal information we may hold, in addition to the information listed on pages 2 to 4, are:

- Address including Residential Address and Postal Address;
- Personal Identification Number (PIN) issued by the Kenya Revenue Authority;
- National security number;
- National hospital insurance number;
- Police clearance;
- Pre-adoptive leave; and
- Compassionate leave.

The table below shows the lawful basis under the KDPA for each of the situations in which we will use your personal information as set out on pages 4 - 8

Purpose / situation	Examples of data involved	Our lawful basis for processing
Checking you are legally entitled to work in relevant countries, and other similar purposes	Right to work evidence, such as copies of passports and / or birth certificates	s. 30(b)(ii) of the KDPA
Making a decision about your recruitment or appointment, and other compatible purposes	References, information included in an application form, CV or covering letter, notes taken at interviews, training records, professional memberships and similar	s. 30(b)(i) of the KDPA
Assessing qualifications for a particular job or task, including decisions about promotions, as well as other similar purposes	As above plus performance information	s. 30(b)(i) of the KDPA
Determining the terms on which you work for us, and other compatible purposes	Contracts of employment and any amendments to them, employment history (including job titles, work history, working hours, holidays), compensation history, tax assessment and similar	s. 30(b)(ii) of the KDPA
Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions, and other compatible purposes	First and last name, PIN number, National security number, National hospital insurance fund number, address, bank account details, payroll records, tax status. Salary, annual leave, pension details, attachment of earnings deductions e.g. child support, employee benefits information and similar	s. 30(b)(i) of the KDPA or s. 30(b)(ii) of the KDPA

Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties and liaising with your pension provider and any other provider of employee benefits, and other compatible purposes	First and last name, date of birth, gender, National Insurance number, details of any additional persons for whom contact details are required, such as your nominated beneficiaries and similar	s. 30(b)(ii) of the KDPA
To manage attendance and timekeeping, and similar purposes	System records for the devices colleagues use to clock in and out of work and similar	s. 30(b)(i) of the KDPA or s. 30(b)(ii) of the KDPA or s. 30(b)(iii) of the KDPA
Business management and planning, including accounting and auditing and compatible purposes	Payroll records, tax status, salary, other payments and similar	s. 30(b)(ii) of the KDPA
Conducting performance reviews, managing performance and determining performance requirements and similar purposes	Appraisal / performance review forms, feedback, information relating to absences, training records, disciplinary, grievances and any other employment matters	s. 30(b)(i) of the KDPA
Making decisions about salary reviews, remuneration and similar purposes	Salary information, salary history, appraisal / performance reviews, feedback and similar	s. 30(b)(i) of the KDPA
Ensuring a safe and secure environment, to prevent and detect crime, disciplinary proceedings and to investigate accidents and incidents, and other similar purposes	CCTV footage, images from CCTV, accident information, 'near miss' information, drug and alcohol testing and similar	s. 30(b)(i) of the KDPA or s. 30(b)(ii) of the KDPA or s. 30(b)(iii) of the KDPA
Gathering evidence for possible grievance or disciplinary hearings and other compatible purposes	Where relevant, statements from witnesses, social media, information relating to absences, training, disciplinary matters, grievances and any other employment matters, photographs and video from CCTV, data on computer network and email use (including data obtained from cookies, web logs and other similar technologies), time and attendance data, alcohol and drugs testing data, and accident/ incident data and similar	s. 30(b)(i) of the KDPA or s. 30(b)(ii) of the KDPA or s. 30(b)(iii) of the KDPA

Making decisions about your continued employment or engagement and compatible purposes	Probation, appraisal and performance review forms, feedback, evidence gathered in relation to grievance, disciplinary or any other employment matters	s. 30(b)(i) of the KDPA
Making arrangements for the termination of our working relationship, and other compatible purposes	Contracts of employment and any amendments to them, start date and, if different, the date of your continuous employment, employment records, appraisal / performance review forms and records and evidence gathered in relation to any employment matters	s. 30(b)(i) of the KDPA
Education, training and development requirements, and other similar purposes	Recruitment records, training records and records and evidence gathered in relation to grievance, disciplinary and any other employment matters, appraisal and / or performance review forms, feedback etc.	s. 30(b)(i) of the KDPA
Dealing with legal issues and situations involving you, or other employees, workers and contractors, including accidents at work	Where relevant, statements from witnesses, social media, information relating to absences, training, disciplinary matters, grievances and any other employment matters, photographs and video from CCTV, data on computer network and email use (including data obtained from cookies, web logs and other similar technologies), time and attendance data, alcohol and drugs testing data, and accident and incident data and similar	s. 30(b)(ii) of the KDPA or s. 30(b)(iii) of the KDPA
Complying with health and safety and associated obligations	Information about accidents and 'near misses' to allow us to investigate the causes and prevent reoccurrence and similar	s. 30(b)(ii) of the KDPA or s. 30(b)(iii) of the KDPA
Monitoring use of IT systems, network and equipment to ensure compliance with our IT policies, and other compatible purposes	Information about how you use our computer network and email service, as well as work equipment such as laptops and mobile phones (including the data obtained from cookies, web logs and other similar technologies) and similar	s. 30(b)(ii) of the KDPA

Information security, including preventing unauthorised access to our computers, systems and network, and to prevent malicious software distribution, and other compatible purposes	Information about how you use our computer network and email service, as well as work equipment such as laptops and mobile phones (including the data obtained from cookies, web logs and other similar technologies) and similar	s. 30(b)(ii) of the KDPA
Data analytics studies to review and better understand employee retention and attrition rates, and other compatible purposes	Leaving date, reason for leaving and similar	s. 30(b)(i) of the KDPA
Business continuity purposes following the cessation of your employment for any reason, including to allow us to ensure that any emails received by you are responded to and any projects you have been involved in can continue to progress	<ul style="list-style-type: none"> • Leaving date • Information about how you use our computer network and email service, as well as work equipment such as laptops and mobile phones (including the data obtained from cookies, web logs and other similar technologies) • The contents of emails addressed to you • The contents of documents contributed to by you 	s. 30(b)(iii) of the KDPA

In addition to the purposes listed on page 9 for how we process sensitive personal information, we may also process special categories of personal information to comply with laws and other measures designed to protect or advance persons or categories of persons disadvantaged by unfair discrimination.

The table below shows the lawful basis under KDPA for each of the situations in which we will process your sensitive personal information as set out on pages 10 and 11.

Purpose / situation	Examples of data involved	Our lawful basis for processing
To ensure your health and safety in the workplace, to provide appropriate workplace adjustments and similar purposes	Information about your physical or mental health, or disability status, medical certificates, GP correspondence and GP and occupational health reports	s. 30(b)(ii) of the KDPA or s. 30(b)(iii) and s. 45 (c) (iii) of the KDPA
Assessing your fitness to work, to monitor and manage sickness absence and other similar situations	Information about your physical or mental health, or disability status, records of sickness and other absences, medical certificates, GP and occupational health reports and correspondence	s. 30(b)(i) of the KDPA and s. 45 (c) (iii) of the KDPA

To administer statutory maternity pay, statutory sick pay, your pension and health insurance, and similar situations	Information about your physical or mental health, or disability status, records of sickness and other absences, medical certificates, GP and occupational health reports and correspondence	s. 30(b)(ii) of the KDPA and s. 45 (c) (ii) of the KDPA
If you wish to join any eligible company life insurance policy or similar, we will process information about your health	Information about your physical or mental health, or disability status, records of sickness and other absences, medical certificates, GP and occupational health reports and correspondence	s. 30(b)(i) of the KDPA and s. 45 (c) (ii) of the KDPA
Health and safety obligations	Information about accidents and 'near misses' to allow us to investigate the causes and prevent reoccurrence	s. 30(b)(ii) of the KDPA and s. 45 (c) (iii) of the KDPA
If we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental or emotional harm or to protect physical, mental or emotional well-being	Information about your physical or mental health, or disability status	s. 30(b)(iii) of the KDPA and s. 45 (c) (iii) of the KDPA
Equal opportunities monitoring	Information about your ethnic group and nationality to ensure meaningful monitoring and reporting	s. 30(b)(ii) of the KDPA and s. 45 (c) (iii) of the KDPA
Biometric data to enable employees to securely log onto their laptops or mobile devices	Biometric Identifiers (such as fingerprint and facial representations) used for secure log in to devices (where consent is given), such as MS Hello.	s.30(1)(a) of the KDPA and s. 45 (c) (ii) of the KDPA

Colleagues who normally reside in Kenya have the right to complain to the Office of the Data Protection Commissioner ("ODPC"). The process is currently set out on the regulator's website here: <https://www.odpc.go.ke/file-a-complaint/>

Colleagues can of course contact the IPL Legal and Compliance team by e-mailing Dataprotection@ipl-ltd.com if they have any questions about data protection or wish to exercise any of their rights.