

# Hilton Foods Privacy Statement

(Generic - Website Users, Candidates, Customers, and Investors)

## Introduction

Hilton Food Group plc and its subsidiary companies (collectively known as 'Hilton Foods' & 'we/our/us') conduct all our business with honesty and are committed to acting professionally, ethically and with integrity in all our relationships. This is a group-wide Privacy Statement which applies throughout our international network.

This Privacy Statement explains how we use your personal data when dealing with Hilton Foods. **This Privacy Statement applies to the personal data of our website users, Candidates, Investors, Customers, Employees, and other individuals we interact with.**

As a Data Controller we comply with applicable data protection legislation across our international network, including but not limited to (i) EU General Data Protection Regulation ((EU) 2016/679) ('EU GDPR'); (ii) UK General Data Protection Regulation (as defined in The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) ('UK GDPR'); and (iii) UK Data Protection Act 2018, and any subsequent legislation when handling your personal data (the 'UK Data Protection Law').

We reserve the right, at our discretion, to change, modify, add, or remove portions of this Privacy Statement at any time. Please regularly check the privacy statement for any changes, this would be signified by the last updated date. Please take time to read this Privacy Statement carefully and get in touch with us if you have any questions or concerns.

## Contact Us

If you have any questions, comments, or concerns about our Privacy Statement, you may email us at [data.controller@hiltonfoodgroup.com](mailto:data.controller@hiltonfoodgroup.com). Additionally feel free to send correspondence to the following address:

For the attention of The Data Controller,  
c/o The Company Secretary,  
Hilton Food Group plc,  
2-8 The Interchange, Latham Road,  
Huntingdon,  
Cambridgeshire,  
PE29 6YE.

## What personal data do we collect?

We may collect and process the following types of personal data:

- **Personal Identification Information:** Name, email address, phone number, postal address, date of birth, national insurance number, gender, photographs, copies of passport or other photo id, copies of proof of address documents (e.g., bank statements or bills), marital status, next of kin or emergency contact information.
- **Employment Information:** Employment history (e.g., job application, employment references, secondary employment), salary and benefits, education history, right to work information, performance records (e.g., reviews, disciplinary records, complaints,), training history and development needs.
- **Sensitive personal information for staff recruitment, administration, and management:** Racial or ethnic origin, political opinions, philosophical beliefs, trade union membership, genetic information, biometric information, health information, sex life information, or sexual orientation information.
- **Security and Compliance Information:** Details of any criminal convictions (e.g., DBS checks), conflict of interest, or gift declarations), monitoring employees' IT use, and CCTV Footage or other recordings.
- **Business Information:** Company name, job title, and business contact details.

Depending on the type of personal data in question and the grounds on which we may be processing it, should you decline to provide us with such data, we may not be able to fulfil our contractual requirements or may not be able to continue with our relationship.

## How do we collect your personal data?

There are three main ways in which we collect your personal data:

- **Directly from you;**
- **From third parties; and**
- **Automatically**

**For all Website Users:** Please refer to ['Website Users' section here](#).

**For Candidates:** We collect personal data in three primary ways:

- 1) **The personal data that you give us**  
By uploading your CV onto the Hilton Foods website, by emailing it to a Hilton Foods employee, or applying for jobs through a third-party website.
- 2) **The personal data that we receive from other sources**

Any references may disclose personal data about you, or we may obtain information from searching potential candidates on third party sources such as LinkedIn and other sites.

**3) The personal data that we collect automatically**

To the extent that you access our website or read or click on an email from us, we may also collect your data automatically or through you providing it to us. Please refer to the [website users section below](#).

**For Customers:**

**1) The personal data that we receive from you directly**

Where you contact us proactively, usually by phone or email; and/or where we contact you either by phone or email, or through our business development activities.

**2) The personal data that we receive from other sources**

We may seek more information about you or your colleagues from other sources by way of due diligence or other market intelligence including:

- From third party market research
- From delegate lists at relevant events
- From publicly available internet and social media sites.
- From third party agencies such as credit reference agencies; and
- From providers of third-party due diligence screening to ensure compliance with our legislative responsibilities and compliance programmes

**3) The personal data that we collect automatically**

To the extent that you access our website or read or click on an email from us, we may also collect your data automatically or through you providing it to us.

**For Employees:**

**1) The personal data that we receive from you directly**

Where you have provided the information during the hiring process, through onboarding forms, or through our administrative activities. Employees may also update their personal data as needed, such as changes in address, marital status, or contact details. Regular performance reviews, training records, and health and safety assessments are other instances where personal data is collected directly from employees.

**2) The personal data that we receive from other sources**

Where appropriate and in accordance with any local laws and requirements, we may seek more information about you or your colleagues from other sources by way of due diligence or other necessary checks including:

- Employment agency
- Schools, colleges, universities, or other education organisations

- Referees (external or internal)
- Occupational Health and other health providers
- Pension administrators or government departments (e.g. HMRC and DWP)
- Trade Unions
- Staff benefit providers
- Public sources (e.g. LinkedIn or other websites)

### **3) The personal data that we collect automatically**

We may collect your data automatically through your use of our internal systems, when you read or click on an email from us or CCTV footage or other recordings.

#### **For Other People:**

##### **1) The personal data that we receive from you**

When you contact us by phone, we collect digital caller information, or by email, we collect your email address. We may note the substance of conversations and contact details where actions arising from the telephone contact are required, you will be notified if this is the case.

#### **People who visit our sites:**

When you visit Hilton sites we will collect your name, company contact information, and relevant health and food safety questions. Please also refer to the '[Site Monitoring Statement](#).'

## How do we use your personal data?

**For Website Users:** Please refer to the '[Website Users](#)' Section [here](#).

#### **For Candidates:**

The main reason for using your personal details is to help you find employment or other work roles that might be suitable for you within Hilton Foods. Where appropriate and in accordance with local laws and requirements, we may also use your personal data for things like:

- Storing your details (and updating them when necessary) on our database, so that we can contact you in relation to recruitment;
- Enabling you to submit your CV or apply online for jobs;
- Verifying details you have provided, using third party resources (such as psychometric evaluations or skills tests), or to request information (such as references, qualifications and potentially any criminal convictions, to the extent that this is appropriate and in accordance with local laws); and
- Complying with our legal obligations in connection with the detection of crime.

Some of the data you may provide and we therefore (in appropriate circumstances and in accordance with local law and requirements) collect about you comes under the umbrella of "diversity information". This could be information about your ethnic background, gender, disability, age, sexual orientation, religion or other similar beliefs, and/or social-economic background.

For some vacancies, we may advertise through a recruitment agency or executive search organisation. We will require them to manage your data in accordance with the GDPR, or the relevant local data protection and privacy legislation. We will remove your information in line with the local data retention policy.

### **For Customers:**

The main reason for using information about customers is to ensure that the contractual arrangements between us can be properly implemented so that the relationship can run smoothly.

We have listed below the several ways in which we use your data in order to facilitate this.

- Storing your details (and updating them when necessary) on our database so that we can contact you;
- Keeping records of our conversations and meetings, so that we can provide targeted services to you;
- Undertaking customer satisfaction surveys;
- To share suppliers' details with retail customers and third parties for supply chain visibility, ensuring the traceability and provenance of food products; and
- We may share your personal data with Credit Reference Agencies (CRAs) to conduct credit checks. CRAs provide us with information such as your financial history, which we use to assess your suitability, verify your identity, manage your account, recover debts, and prevent criminal activity. We will continue to share information with CRAs, including details of settled accounts and unpaid debts.

### **For Other People:**

If a candidate or employee has provided your details for an emergency contact, we will contact you in the case of an accident or emergency affecting them; or

If you were put down as a referee, we will contact you to take a reference. This is an important part of our recruitment process and could be the difference between the individual getting a job or not.

### **For Employees:**

We use your data in the following ways:

- Recruitment
- Administration
- Management

- Training and performance reviews
- Payroll
- Employee Benefit Schemes

### **Payroll**

Where we outsource payroll, we will provide the payroll company with the details required for them to process your pay and to send you tax summaries. Where there is a provider involved, they will be the data processor. They are required to adhere to Hilton Food's data protection policies. Please refer to the local People and Culture contact for details of your payroll service.

### **Hilton Food's Employee Share Schemes**

The administrators of the Hilton Food's share schemes function as processors of personal data to manage your membership of the scheme. The administrators are contractually bound by Hilton Foods as a processor. For UK and Europe the Equiniti Privacy Statement is available [here](#). For APAC the Link privacy statement is available [here](#).

### **Other third parties**

For all the companies Hilton Foods partners with for people and culture services, for example training and benefits providers, they will be the data processor. They are required to adhere to Hilton Food's data protection policies. Please refer to the local People and Culture contact for details.

## **How do we safeguard your personal data?**

We are committed to taking all reasonable and appropriate steps to protect the personal data that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures for example data protection policies and IT security procedures.

If you suspect any misuse or loss of or unauthorised access to your personal data, please let us know immediately. Details of [how to contact us is here](#).

## **How long do we keep your personal data for?**

We retain your personal data for as long as necessary to fulfil the purposes outlined in this Privacy Statement unless a longer retention period is required or permitted by law.

We will not hold your personal data for longer than is necessary. The length of the retention period will be in accordance with the local data retention policy, which will be dependent on the following circumstances:

- The end of the relationship
- The completion of the purpose for which the personal data was given.
- Our legal obligations in relation to that personal data
- The type of data

## How you can access, amend, or take back your personal data?

You retain specific rights over your personal data, even after sharing it with us. These rights are designed to protect your privacy and give you control over your information.

- **Right to be informed:** You have the right to know why personal data is collected and what will be done with it. By this privacy statement we are informing individuals what data we are collecting and for what purpose.
- **Right of access:** You can request what information we hold about you, as well as why we have that information, who has access to the information and where we got the information.
- **Right to correct and update:** If the data we hold about you is out of date, incomplete or incorrect, you can inform us, and we will ensure that it is updated.
- **Right of erasure:** If you feel that we should no longer be using your data, or that we are illegally using your data, you can request that we erase the data we hold. We will confirm whether the data has been deleted or tell you the reason it cannot be deleted.
- **Right to restriction:** You have the right to require us to restrict processing of your personal data under certain circumstances.
- **Right to data portability:** You have the right to transfer your data from one data controller to another. We must either give you a copy of your data or transmit it directly to the new data controller.
- **Right to object or withdraw consent:** You have the right to request that we stop processing your data. We will confirm if we are able to comply with your request or if we have legitimate grounds to continue. If data is no longer processed, we may continue to hold your data to comply with your other rights.
- **Rights related to automated decision-making including profiling:** You have the right to not be subject to decisions made solely on automated processing, including profiling, which significantly affects you. You can request human intervention, express your point of view, and contest the decision.

### How to Exercise Your Rights

[You can read more about these rights here.](#) For any requests or questions about your rights, please [contact us here](#). We may need proof of identity to confirm the request. Note that we may keep a record of communications to help address any issues. Rest assured, we will respond promptly within one month and explain if there are any reasons we cannot comply with your request.

## The lawful basis of processing your personal data

We process your personal data based on the following legal grounds:

- **Consent:** We process your data with your explicit consent, provided after giving you all relevant information. While most of your data protection rights apply, including the right to withdraw consent at any time, please note that the right to object does not apply in this context.
- **Contractual Necessity:** Processing is required to fulfil a contract we have with you, or to take steps at your request before entering a contract.
- **Legal Obligation:** We process your data when necessary to comply with legal obligations.
- **Preventing Worker Exploitation and Modern Slavery:** To detect and prevent worker exploitation and modern slavery, safeguarding potential victims and complying with related legal obligations.
- **Legitimate Business Interests:** We may process your data for our legitimate business purposes, provided your rights do not override these interests. This includes:
  - Providing the information, products, and services you request (e.g., processing deliveries).
  - Notifying you of changes to our services.
  - Ensuring our website content is displayed in the most user-friendly way.
  - Communicating with you to provide requested information or resolve issues, including managing complaints and disputes.
  - Maintaining the health, safety, and welfare of our employees, business partners, and suppliers.
  - Training and other People and Culture related activities
  - Keeping our website secure.
  - Improving and developing new products and services.
  - Handling legal or insurance claims, as well as regulatory actions.
  - Managing corporate transactions such as acquisitions, transfers, or sales of businesses.
  - Investigating or responding to complaints or ethical concerns raised by or involving you.
  - Preventing, detecting, or investigating criminal activity, including working with law enforcement agencies where necessary.
- **Vital interests:** Collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an



urgent need for life sustaining food, water, clothing, or shelter. All your data protection rights may apply, except the right to object and the right to portability.

## Sharing and Transferring your Personal Data

We may share your personal data with a variety of individuals and organisations for specific reasons. The categories of people we may share your data with include:

1. **Group Companies:** Any of our subsidiary companies.
2. **Reference and Application Contacts:** Individuals and organisations involved in your reference or job application process, such as past, current, or prospective employers, educators, examining bodies, and recruitment agencies.
3. **Authorities and Regulators:** Tax, audit, or other authorities when required by law or regulation (e.g., requests from tax authorities or in anticipation of legal proceedings).
4. **Third-Party Service Providers:** External consultants, business associates, and professional advisers (including lawyers, auditors, accountants), as well as technical support teams and IT consultants for system testing and development.
5. **Background Check Providers:** Third-party providers conducting reference, qualification, and criminal record checks where permitted and in line with local laws.
6. **Business Transfers:** In the event of a merger or acquisition, or meaningful discussions regarding such actions, your data may be shared with the prospective owners of the business.

### Personal Data Transfers

Your personal data may be transferred within and outside of our international network. Where such transfer is required, your personal data will be subject to appropriate safeguards, in accordance with the relevant data protection laws, both within and outside of the European Economic Area (EEA). These safeguards may include:

1. **Internal Data Protection Framework:** Hilton Foods have rules which include all general data protection principles and enforceable rights to ensure appropriate safeguards.
2. **Adequacy Decisions:** Hilton Foods will only transfer your personal data to countries where privacy laws ensure an appropriate level of protection as signified by the adequacy decisions.
3. **Data Transfer Agreements:** Hilton Foods will have data transfer agreements when entering contracts with third parties so that your personal data is protected to the same standards as stipulated by GDPR.

4. **Contractual Necessity:** In cases where data transfer is required to fulfil or perform a contract in your interest, such as if you are a client and the transfer is necessary to meet contractual obligations.
5. **Your Consent:** If you have explicitly consented to the transfer of your data outside the EEA.

If you would like more details or a copy of the specific safeguards applied to any transfer, please [contact us using the details provided here](#).

## Website Users

When you visit our website there is certain information that we may automatically collect, whether you decide to use our services. This includes your IP address, the date, times, and frequency with which you access the website and the way you browse its content. We will also collect data from you when you contact us via the website, for example when downloading or requesting a report.

### Use of Third-Party Services

When someone visits <https://www.hiltonfoods.com/> we use a third-party service, Google Analytics, to collect standard internet log information and details of visitor activity patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way that does not identify anyone.

We use a third-party service to help maintain the security and performance of our website. To deliver this service it processes the IP addresses of visitors to the Hilton Foods website but does so passively by not recording any personal data.

Search queries and results are logged anonymously to help us improve our website and search functionality. No user-specific data is collected by either Hilton Foods or any third party. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website. If we do want to collect personally identifiable information through our website, we will let you know about this. We will make it clear when we collect personal data and will explain what we intend to do with it.

### Use of Cookies

A "cookie" is a bite-sized piece of data that is stored on your computer's hard drive. They are used by all websites and do not harm your system. We use them to track your activity to help ensure you get the smoothest possible experience when visiting our website. We can use the information from cookies to ensure we present you with options tailored to your preferences on your next visit. We can also use cookies to analyse traffic and for advertising purposes.

You can read more about how we use cookies on our [cookies page](#). You also have the option to set your own cookies settings from the menu at the bottom of our website.

### Links to other websites

This privacy statement does not cover the links within this site linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

We may also use third parties to provide apps, tools, widgets, and plug-ins for our online services, which may collect information about how you use these features. These organisations have their own privacy policies, and we would again encourage you to visit their websites and view the privacy policies.

## Investors

Hilton Foods does not directly process any personal data from investors and uses Equiniti as registrar. Equiniti's privacy statement is found [here](#).

## Site Monitoring Statement

We have CCTV cameras installed for security, safety, and access control. It is therefore only in public areas, and not in the changing room or toilets, or anywhere else expected to be private. Access to this footage is restricted to authorised persons and will only be accessed in the event of a suspected breach of the above. Please refer to local CCTV policies for more details.

We have time recording, which identifies individuals for the purposes of ensuring that people are properly paid, to flag absence issues and to facilitate complete evacuation in the event of a fire. Please refer to the local People and Culture department for more information.

The Group has common IT security policies and server profiles that actively monitor the IT environment to ensure its security and proper use. Activity can be traced back to individuals by way of event logs, email records and telephone logs. Logs are kept securely and have limited access by staff. Records and logs are destroyed in line with data retention policy.

The IT Policies explain what users can and cannot do with IT and communications equipment and should you have any questions then please refer these to the local IT contact.

Hilton will use computer files and other records to investigate any suspected illegal activity or unacceptable behaviour in line with our policies and procedures with the approval and overview of senior management. Monitoring activity has legal implications in terms of privacy, data security and personal rights. The purpose of monitoring is for safety and for compliance with company policy, and relevant laws and regulations.

## Complaints or queries

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy statement. The Data Controller is obliged to record and to respond to your complaint.

If you remain unhappy with how we have used your data after raising a complaint with us, you can also complain to the ICO or relevant local authority.

The ICO's address:

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Helpline number: 0303 123 1113

Website: <https://www.ico.org.uk/make-a-complaint>

## Contact Local Data Protection Authorities

Please consult and comply with applicable local laws in the European Economic Area (EEA), Australia, New Zealand, USA, Canada, and China, as these regions may have specific requirements or additional obligations that must be met in conjunction with our UK GDPR-compliant policy.

- Australia: Privacy Act 1988
- Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)
- China: Personal Information Protection Law (PIPL)
- New Zealand: Privacy Act 2020
- USA: US-UK Data Privacy Framework

### Australia

Office of the Australian Information Commissioner (OAIC)  
Address: GPO Box 5218, Sydney NSW 2001, Australia  
Email: [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)

### New Zealand

Office of the Privacy Commissioner (OPC)  
Address: PO Box 10094, Wellington 6143, New Zealand  
Email: [enquiries@privacy.org.nz](mailto:enquiries@privacy.org.nz)

### China

Cyberspace Administration of China (CAC)  
Address: 225 Chaoyangmen Nei Dajie, Dongcheng District, Beijing 100010, China  
Email: [cac@cac.gov.cn](mailto:cac@cac.gov.cn)

**Canada**

Office of the Privacy Commissioner of Canada (OPC)  
Address: 30 Victoria Street, Gatineau, Quebec K1A 1H3, Canada  
Email: [info@priv.gc.ca](mailto:info@priv.gc.ca)

**Denmark**

Danish Data Protection Agency (Datatilsynet)  
Address: Carl Jacobsens Vej 35, DK-2500 Valby, Denmark  
Email: [dt@datatilsynet.dk](mailto:dt@datatilsynet.dk)

**Ireland**

Data Protection Commission (DPC)  
Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland  
Email: [info@dataprotection.ie](mailto:info@dataprotection.ie)

**Portugal**

Comissão Nacional de Proteção de Dados (CNPd)  
Address: Rua de São Bento, 148, 3º, 1200-821 Lisboa, Portugal  
Email: [geral@cnpd.pt](mailto:geral@cnpd.pt)

**Sweden**

Integritetsskyddsmyndigheten (IMY)  
Address: Box 8114, 104 20 Stockholm, Sweden  
Email: [imy@imy.se](mailto:imy@imy.se)

**Netherlands**

Autoriteit Persoonsgegevens (AP)  
Address: PO Box 93374, 2509 AJ The Hague, Netherlands  
Email: [info@autoriteitpersoonsgegevens.nl](mailto:info@autoriteitpersoonsgegevens.nl)

**USA**

Federal Trade Commission (FTC)  
Address: 600 Pennsylvania Avenue, NW, Washington, DC 20580, USA  
Email: [webmaster@ftc.gov](mailto:webmaster@ftc.gov)

**Poland**

Urząd Ochrony Danych Osobowych (UODO)  
Address: Stawki 2, 00-193 Warsaw, Poland  
Email: [kancelaria@uodo.gov.pl](mailto:kancelaria@uodo.gov.pl)

**Spain**

Agencia Española de Protección de Datos (AEPD)  
Address: Jorge Juan, 6, 28001 Madrid, Spain  
Email: [internacional@aepd.es](mailto:internacional@aepd.es)