

## Hilton Food Group Privacy Statement

Hilton Food Group and its subsidiary companies respect personal privacy and will process any personal information only for the purpose it is intended. We will never sell your personal information to third parties and will work hard to ensure compliance with all privacy law including the General Data Protection Regulations.

### How we use your information

This Privacy Statement tells you how we use **your** personal data when dealing with Hilton Food Group or its subsidiaries.

We have provided specific information for visitors to this site and to job seekers or employees

- [Visitors to our website](#)
- [Job applicants and employees](#)
- [Investors](#)

### Privacy Management and How to Contact Us

Hilton Food Group has appointed data controllers within each of its subsidiaries as the person responsible for ensuring procedural responsibility for its legal obligations over data security and privacy.

Contact details for each site are listed on their respective websites.

The Data Controller for the UK Group Head Office can be contacted at:

[data.controller@hiltonfoodgroup.com](mailto:data.controller@hiltonfoodgroup.com)

The Data Controller  
c/o The Company Secretary  
Hilton Food Group plc  
2-8 The Interchange  
Latham Road  
Huntingdon  
Cambridgeshire  
PE29 0YE

## Complaints or queries

If you want to make a complaint about the way we have processed your personal information, you can contact the Data Controller who is obliged to record and to respond to your complaint. The principal controller for the purposes of the GDPR implementation is the UK Information Commissioner.

To report a concern to the UK Data Commissioner then you can do so at this site:

<https://ico.org.uk/concerns/>

## Links to other websites

This privacy notice 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. These other websites would relate to external processors of your personal data.

## Changes to this privacy notice

We keep our privacy notice under regular review. This privacy notice was last updated on 27 April 2018.

## Visitors to our websites

When someone visits [www.hiltonfoodgroup.com](http://www.hiltonfoodgroup.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 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 be up front about this. We will make it clear when we collect personal information and will explain what we intend to do with it.

## Use of cookies by the Hilton Food Group

You can read more about how we use cookies on our [cookies page](#).

## Search engine

Our website search and decision notice search is powered by System Associates. 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 Food Group or any third party.

## Security and performance

Hilton Food Group uses 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 Food Group website but does so passively.

## People who call us by phone

When you contact us by phone we collect digital caller information. We use this information to help improve its efficiency and effectiveness of our systems and do so passively. We may note the substance of conversations and contact details where actions arising from the telephone contact are required.

## People who email us

We encrypt and protect email traffic. If your email service does not support encryption, you should be aware that any emails we send or receive might not be protected in transit.

We will also monitor any emails sent to us, including file attachments, for viruses or malicious software. Please be aware that you have a responsibility to ensure that any email you send is legal. Internet routing may result in data being moved outside of the European Union.

## Site Visitors

Visitors to site will need to identify themselves and we will hold their name and company contact for the duration of the visit.

## Job applicants and employees

Hilton Food Group is the data controller for the information you provide during the recruitment and employment process unless otherwise stated. If you have any questions relating to the process or any privacy or data security issues then please raise these with your HR or recruitment contact.

## What will we do with the information you provide to us?

All of the information you provide during the process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the recruitment process with any third parties or store it outside of the European Economic Area. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for.

## What information do we ask for, and why?

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary. For unsuccessful applicants we will delete your record straight away.

The information we ask for is used to assess your suitability for employment – this assessment is not done automatically. You do not have to provide what we ask for but it might affect your application if you do not. We could request you to provide information verbally, by letter, email or social media.

During the application course we will ask you for personal information such as name, address, date of birth, gender, National Insurance or Social Security Number email address and phone numbers.

We will ask you for proof of identity to satisfy our right to work verification obligations. This would include national ID Card, driving license, Immigration Department letter or passport copy showing name page and visa page. We may ask for a letter confirming National Insurance Number from the Government Department to allow us to confirm your right to work in the EU and we may ask for any tax forms relating to previous employment so that we can deduct the correct income tax from your earnings. We would ask for education certificates, and work history to satisfy suitability for role questions. For all of these, we would request original documents to be seen by us prior to confirming a contract of employment. We will make a copy of those documents and keep them until we are no longer obliged to fulfil employment obligations.

We may make pre-employment checks by asking for references, their contact details, and the context and employment history to verify the roles you had been employed in.

We may ask you to provide health information that would be processed by an occupational health organisation to assess your suitability for role. The privacy policy of this company is [here](#).

Following your application, we would ask for bank account details in order for us to pay your salary and name and contact details for emergency contact. We would pass these to a payroll processor within the company or an outsourced provider.

If you were entitled to medical insurance then we would provide you with a form for you to fill in giving personal details. We would not hold a copy of this but might hold a record of providing you with this entitlement. If you were covered by a company insurance policy then we may ask for a named beneficiary for the purpose of administering any payment.

We may send some of your personal data to a company to provide you with pensions savings whose privacy statement can be [found](#)...

We will ask for or take a photograph to be used on email and electronic systems time monitoring for identification purposes and for processing time based payment and a fingerprint for automated access systems. We will destroy these when you leave the company.

During the course of your employment, we will ask you to complete forms with personal data for the purposes of booking holiday and informing of absence.

#### Payroll:

Where we outsource payroll we will provide the payroll company of your name, bank details, national insurance number and your address for them to process your pay and to send you tax summaries by post. The privacy statement of this company is [here](#).

#### Sharesave Scheme:

The Company Sharesave Scheme is administered by Equinity who act as a processor of personal information to manage your membership of the scheme. Equinity are contractually bound by Hilton Food Group as a processor. Their Privacy Statement is found [here](#).

#### Recruitment Agencies

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. We will not retain any personal data provided if you are not successful as an applicant.

#### Site Contact:

Employees should contact their HR Department to discuss any issues of Data Protection.

#### Data Retention

All computer and paper archives of the company will be destroyed within 7 years.

For employee personal data then their file will be removed from the processing environment immediately after their leaving date or as soon as practically after that. This includes training information and payroll and attendance data too. There may be a requirement to subsequently process personal information such as for year-end tax returns but after those overriding reasons have expired then the persons personal data will be removed.

For job applicants data will only be retained on confirmation of a contract of employment.

## Your Rights:

You have rights under European legislation commonly referred to as the GDPR – General Data Protection Regulations. Hilton Food Group applies the principles underlying data protection law in all of its subsidiary companies and complies with all relevant legislation relating to privacy and the retention of personal information. This section applies to all people whose personal data is held by Hilton.

Specifically you have rights to ensure that the personal data that you have provided to us is treated correctly, for the purpose it has been given and according to the law – in particular the law commonly described as the General Data Protection Regulations – GDPR.

The legal basis for processing personal data will in order to fulfil a contract of employment or supply of goods or services.

You have the right to see all the personal data referring to you. This includes the right to access data within a month of a request being made. You have the right to be given that data in a form that is 'portable'. This means that we will supply you it in common format such as .pdf, word, .txt or other commonly used formats to ensure its portability – so that you can take it with you and use it elsewhere. The format and context can be discussed with the Data Controller should you make a request for data access.

You have the right to have any data that is incorrectly recorded rectified promptly.

Where the legal basis of processing information is by specific consent then you have the right to withdraw consent at any time. Within Hilton Food Group, virtually all data processing will be carried out in relation to the operation of a contract of employment or supply and Hilton Food Group will not normally use consent as the legal basis for processing data. If you wish to withdraw consent then you can do this with your data controller.

Equally, you can have the right to restrict the content of the personal data that we process and this can be discussed with the controller and arrange for it to be removed if it is not needed.

You have the right to erasure. Commonly described as the 'right to be forgotten' you can request that your personal data is erased. In practice, this means that we will, upon request, cease to process personal data. We will offer you the opportunity to discuss how this will be done when you request your data be erased. In some circumstances, data will still be held – for example if there is a legal obligation requiring continuing data storage – such as with Tax authorities. However all other processing will stop and full erasure will follow the expiry of the overriding legal obligation.

Personal information will not be transferred outside of the European Union other than subject to the strict controls that the Group is required of by in complying with national data privacy and security law.

In matters of privacy and data security there are established routes to make complaints and to escalate any issues outside of the company. The process for making a complaint is through the local HR. You can make a complaint to the local data Commissioner and should note that because of the structure of the Group the principal or lead Data Commissioner is the UK Information Commissioners Office.

#### For Investors:

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

#### Site Monitoring:

Within each of the Hilton Food Group's sites monitoring takes place for reasons connected with the safe operation of the business.

#### Site Monitoring Statement

Within each of the Hilton Food Group's sites monitoring takes place for reasons connected with the safe operation of the business. Clearly, we monitor temperature and physical conditions for the safe and effective operation of the factories and to comply with customer requirements for storage and food management in production. We also monitor the built environment with smoke and fire detection and electrical and ammonia circuits and pressure for safety and security. We have TV cameras installed for security, safety and access control. We have Time Recording, which identifies individuals for the purposes of ensuring that people are properly paid and to facilitate complete evacuation in the event of a fire.

The Group has common IT security policies and server profiles that actively monitor the IT environment to ensure its security and proper use. From monitoring the IT environment is activity can be traced back to individuals by way of event logs, email records and telephone logs. Logs are kept securely and have very 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 your controller.

Hilton will use computer files and other records to investigate any suspected illegal activity or unacceptable behaviour 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.