



PRIVACY NOTICE (EXTERNAL)

Data Controller

Malhotra Group PLC (“we”, “our”, “us”) processes personal data in accordance with our obligations under the General Data Protection Regulations 2016 (“GDPR”) and is a registered Data Controller with the Information Commissioner’s Office (“ICO”), which is the supervisory authority responsible for the oversight and enforcement of Data Protection Legislation within the United Kingdom.

ICO Registration Number: ZA044474

Data Protection Officer

The Data Protection Officer (“DPO”) for the Malhotra Group PLC is Paul Wright. You may contact the DPO if:

- You would like to receive a copy of your data
- You have any questions you feel have not been covered by this Privacy Notice.
- You have any concerns about the processing of your data.
- You wish to make a complaint about the processing of your data.

You can contact our DPO at paul@malhotragroup.co.uk or call 0191 233 0387.

General

This Privacy Notice is a statement that describes how and why we process personal data in relation to an individual. We take seriously our obligation to respect the right to privacy and the protection of personal information. We pledge to handle data fairly and legally and all times.

This notice also explains how you might control the use of your personal data in accordance with your rights under GDPR.

This notice also explains your rights in relation to personal data under GDPR.

Malhotra Group PLC will not disclose your personal data to any unaffiliated third parties. Furthermore, we will never sell or rent our user information to other organisations for external marketing purposes. This privacy notice provides you with information on why we collect your personal information, how we use it, the limited conditions under which we may disclose it to others, and how we keep your information secure.

Malhotra Group PLC use your personal data:

- To verify your identity.
- For market research purposes (for which we will always obtain your consent).

- Where we have a legal right or duty to use or disclose your information (for example in relation to an investigation by a public authority or in a legal dispute).
- For the protection of our employees and users
- For crime and fraud prevention, detection and related purposes.
- To manage any registered account that you hold with us.
- To contact you electronically about promotional offers with your agreement (where you consent has been given).

Types of data we collect

We collect and process various categories of personal information in order to provide our services effectively. This may include (but is not limited to):

- Your name, age/date of birth and gender.
- Your contact details: postal address, telephone numbers and e-mail address.
- Your on-line browsing activities.
- Your password(s).
- Your communication and marketing preferences.
- Your feedback and survey responses.
- Your location.
- Your correspondence and communications with Malhotra Group PLC.
- Other publicly available personal data, including any which you have shared via a public platform (such as Twitter, Facebook, Instagram or LinkedIn).

Our websites are not intended for children, and we do not knowingly collect data relating to children.

This list is not exhaustive, and in specific instances we may collect additional data for the purposes set out in this Privacy Notice. Some of the above personal data is collected directly, for example when you set up an on-line account on our websites, use our Wi-Fi or send an email to an employee within our Group. We may also collect personal data from third parties who have your consent to pass your details to us, or from publicly available sources.

Information may be collected using the following:

Website Cookies

Our websites use cookies to collect information. This includes information about browsing behaviour by people who access our websites. This includes information about pages viewed and the journey around our websites.

What are cookies?

Like most websites, Malhotra Group PLC uses cookies to collect information. Cookies are small data files which are placed on your computer or other devices (such as smart 'phones' or 'tablets') as you browse a website. They are used to 'remember' when your computer or device accesses our websites. Cookies are essential for the effective operation of our websites.

What are cookies used for?

The main purpose for which cookies are used are:

- For technical purposes essential to the effective operation of our websites, particularly in relation to site navigation.

- For Malhotra Group PLC to market to you, particularly banner advertisements and targeted updates.
- To enable Malhotra Group PLC to collect information about your browsing patterns, including to monitor the success of campaigns and competitions etc.

How do I disable cookies?

If you want to disable cookies you need to change your website browsing settings to reject cookies. How this is done will depend on the browser you use.

Google Analytics

When someone visits our websites, we use a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We use limited 'profiling' (where information about you is used to tailor goods or services based on your interests, movement or records of your activities). This information is only processed in a way which 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 websites.

Wi-Fi

When you use Malhotra Group PLC's Wi-Fi, we may collect data about:

- Your device.
- The volume of data which you use.
- The websites and applications which you access.
- Your usage by access time, frequency and location.

Mailing Lists

We store opt-in subscriber information securely via Mailerlite services. The information we collect may include subscribers:

- Name
- Date of birth
- Email address
- Location

We use this information to give you information you have requested us to tell you about. We may also use this information to contact you if we need to obtain or provide additional information. We may also contact you to check our records are correct and that you are satisfied with our services.

Curriculum Vitae

We may obtain information about you when you apply for a job vacancy or when you submit a prospective CV for upcoming or potential vacancies. We will only store this information for a period of 6 months, unless you consent to your information being held for a longer duration. You can withdraw consent for this at any time if you do not wish for us to store your data.

Activities we process your personal data for and the lawful basis

Under Article 6 of GDPR, we must identify a basis for the 'lawfulness of processing' of our activities involving of your data. These are broadly described as: 'Consent', 'Contract', 'Legal Obligation', 'Vital Interests', 'Public Interest (or Public Task)' and 'Legitimate Interests'.

When joining us

Where you have 'given consent to the processing of personal data for one or more specific purposes' you can withdraw consent for or object to at any time.

These activities have been identified as processing where it is 'necessary for the purposes of the legitimate interests pursued by the controller' (us) or you, as an enquirer or where you have 'given consent to the processing of personal data for one or more specific purposes' which you can withdraw consent for or object to at any time:

- Company activities and events organised for customers and partners in relation to future opportunities or associated material we think might be of interest to you, for example Surveys, feedback and similar communications.
- We may use your data to analyse monitor and evaluate our recruitment effectiveness or other performance and effectiveness in order to maintain and improve our services.
- We may seek your views directly through online questionnaires, invitations to participate in focus groups, or other technology-based surveys.
- Providing a more personalised user experience when using our website or any other services, allowing us to target you with information we think you might be most relevant to you and your enquiries.

Data is also processed for the following activities, which have been identified as necessary 'for us to comply with the law':

- For monitoring compliance with and enforcement of relevant policies in relation to health and safety and security (prevention and detection of crime) which includes the use of CCTV, and safeguarding.
- For compliance with UK Border Agency requirements and for meeting professional statutory regulatory bodies requirements.
- Production of statistical returns required for third party government bodies or for completion of government supported surveys.
- To monitor and promote equality and diversity throughout the Group. This may include the production of non-identifiable statistical data for analysis.

Photographs

Photographs may be taken at our events for use in communications and marketing materials, including on our website and on social media channels. Where you are not the subject of the image (i.e., if it is a 'group' or 'crowd' photograph), we may use such images without requiring your consent, however, where you are the subject of the photograph, you will be asked to provide your explicit consent to use the image. Notifications will be put up in and around these 'open' events to inform you when such photography is taking place. You have the right to object or restrict your image being taken or used. If you would like to exercise this right, please contact our DPO as set out above.

Communications

All communication with you, including in relation to updates to this privacy notice, will, where possible be made via email. If, at any stage, you are concerned about the content (e.g., unwanted marketing), frequency (too many) or method (change preference) of these communications, you can unsubscribe or update your preferences using the link which will be provided at the bottom of the relevant correspondence.

Should you unsubscribe from our marketing messages you will miss regular communications about our services and updates.

How personal data is stored securely by Malhotra Group PLC

We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure. In addition, we limit access to personal data to those employees, agents and contractors that have a legitimate business need for such access. All of our employees, contractors and volunteers with access to personal data receive mandatory data protection training and have a contractual responsibility to maintain confidentiality and access to your data is restricted to those members of staff who have a requirement to access it.

We utilise different storage solutions and IT systems, some of which are outsourced to third party providers. Where processing takes place with an external third party, processing takes place under an appropriate agreement outlining their responsibilities to ensure that processing is compliant with the Data Protection legislation and verified to be secure. Where applicable, any credit/debit card details provided will be stored in full compliance with PCI-DSS requirements.

Once the data is no longer required, the records will go through an appraisal process. This process will determine if there is a continuing legal basis for keeping the record. The DPO will have final responsibility for determining whether the record will be destroyed or retained. The DPO will maintain a record of all retention or disposal decisions.

Data protection by default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

Transfers to third party countries

Where data is shared with third party countries, we ensure that these countries are either approved by the European Commission as having 'adequate protection' or we put in place 'appropriate safeguards' and contracts with these organisations, so as to maintain the security of the data and your rights under relevant Data Protection legislation. There may also be limited sharing with organisations in third countries under specific exemptions, for example, with your explicit consent.

Your Rights under GDPR

Under GDPR, you have a number of rights in relation to the processing of your personal information, each of which may apply to differing degrees' dependent upon the nature of the processing and the legal basis for it. You have the right to:

- Be informed as to how we use your data (via this privacy notice).
- Request access to the personal information that we hold about you.
- Correct inaccurate or incomplete data.
- Request that we stop sending you direct marketing communications.

In certain circumstances, you may also have the right to:

- Ask to have certain data erased by us.
- Request that we restrict certain processing of your personal data.
- Request that we provide any data you submitted to us electronically be returned to you or passed to a third party as a data file.
- Object to certain processing of your personal data by us.

In some cases, there may be specific exemptions as to why we are not able to comply with some of the above. Where this is the case, we will explain the reasons why.

To exercise any of the above rights, please contact our Data Protection Officer (details above).

What to do if there is a security breach

In order to mitigate the risks of a security breach we will follow the Physical Access, Digital Access, Access Monitoring and Data Security Procedures outlined within in the Data Protection Policy. In the instance that it appears that a data security breach has taken place the staff member who notices the breach, or potential breach, will report this incident to their Line Manager, who will subsequently notify the DPO.

In the instance that the breach is a personal data breach and it is likely that there will be a risk to the rights and freedoms of an individual, then the Information Commissioner's Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach, and reported directly to the ICO (<https://www.ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>). The Data Security and Protection Lead will inform any individual that their personal data has been breached if it is likely that there is a high risk to their rights and freedoms. We will inform them directly and without any undue delay.

Lodging a Complaint with the ICO

If you are dissatisfied with our processing of your data, or a response to a complaint you have made to us about it, you have the right to complain to the ICO. The contact details for the ICO are:

Information Commissioner's Office
Wycliffe House Water Lane
Wilmslow Cheshire
SK9 5AF
Telephone: 0303 123 1113 (local rate) or 01625 545 745

For more information you may also visit the Information Commissioner's web site at <https://ico.org.uk/>

Changes to this Privacy Notice

We keep this Privacy Notice under regular review and will communicate any significant updates to you and update our websites accordingly.

This privacy notice was last updated in **January 2026** and will be reviewed at least on an annual basis.