Mi Hub Privacy Policy

Overview

This notice details how the personal data Mi hub collects is stored and used together with details of an individual rights in relation to this information. The notice applies to personal information provided to us directly or by others on an individual's behalf.

Terms

'We' or 'us' as mentioned in this notice refer to Mi Hub Limited (England & Wales registration number: 00454264) and may also refer to individual brand names or subsidiary companies. The terms "you" or "your" refer to you as an individual. This policy covers the following brands and locations (collectively called Mi Hub):

Name & Brand	Address/Contact Information	Registration Number
Mi Hub Limited (for all UK locations): • Dimensions • Alexandra • Yaffy	Data Privacy Office 3 Long Acre, Willow Farm Business Park, Castle Donington, Derbyshire, DE74 2UG 01332 697227 dpo@mi-hub.com	00454264
Alexandra Corporate Fashion BV	Sterrekroos 7 4941 VZ Raamsdonksveer Nederland 01332 697227 dpo@mi-hub.com	50728474

The details above can also be used to contact us in respect of your legal rights under EU GDPR or the UK DPA 2018/UK GDPR.

Types of information collected

In the course of our business activities, it is necessary to collect personal information from our customers and employees. The most common interactions will be around the placing of orders and the marketing of products. The table below highlights the type of interaction and the personal data collected as a result. The data we collect about our employees is contained in our Employee Privacy Policy.

Who we collect from	What personal data we collect
Prospective employment candidates.	Applicant details (CV), including name, contact number and email, previous employment history.
Individual Customers or prospective customers (also Corporate Buyers on behalf of companies)	Login information, names, shipping address, product sizing or modifications to products, delivery contact name if different, payment (credit card for example) details etc., telephone call recordings, online "Live Chat" messages and catalogue requests.
Website Visitors	Technical information (cookies, browser type, and IP address), visits to our websites, whether an order is placed, requests for catalogue or other marketing information requests & newsletter requests
Corporate Customer employees (wearers)	Only if your personal data is provided to us by your employer, do we use that data for sizing, shipping, or order confirmations.

Storage locations of personal data

Mi Hub have premises throughout the UK and an office in the Netherlands (EU). Access to data is maintained from these locations to enable the fulfilment of customer orders and employer responsibilities.

As part of our data security arrangements, we use a UK-based cloud service to hold copies of our business data, providing a robust service to our customers.

In order to provide a smooth browsing experience our websites may be supported by trusted suppliers outside of the EEA with standard data protection contracts in place. This provides safeguards for personal information and ensures compliance with UK and European data protection regulations.

Collection and use of personal information

The purposes for collecting and the further processing of personal data are summarised below:

Category	Lawful Purpose
Account creation, order processing, invoicing/billing, contract obligations from your employer, order information status & updates, customer service.	Execution or performance of a contract
Promotion of Goods similar/connected to your browsing, orders and garment allocation.	Legitimate interest.
Technical information to ensure that the websites perform as needed and technical issues are resolved.	Legitimate interest.
Provision of marketing information (catalogues, newsletters, promotions etc.)	Opt-in consent.
Anonymised data. Using general and statistical data to identify trends or market research.	Legitimate interest.
Regulator requests, government requests etc.	Legal or Regulatory requirement.

Marketing Preferences

Each website offers visitors the opportunity of opting in to receive marketing information detailing goods or services we feel may interest you. Following initial set up, an individual's preferences can be changed through contacting us or making changes on your marketing webpage. It takes up to 48 hours for any changes to take effect.

Telephone Call Recording policy

To enable the fulfilment of our contractual obligations and for quality monitoring, training, compliance, and security obligations a telephone call recording function is in operation.
Inbound and outbound calls involving certain departments (e.g. Customer Services, Sales and Credit Control) may be recorded and retained in accordance with our retention periods. The usage of these recordings is limited to the purposes specified in our Telephone Call Recording policy, which is available across our web sites or upon request. In the event a call is transferred from Sales, Customer Services or Credit Control to a different department the call recording automatically ceases on completion of the transfer.

Security

Data security is paramount and Mi Hub take all appropriate steps to ensure we are meeting our obligations and responsibilities to our customers. The ways in which we achieve this are detailed below:

- **Browser & Web Server**
  We use Transport Layer Security (TLS) to encrypt data transmissions between your browser and our web server, to ensure that all personal and transactional information is protected from eavesdropping, tampering or alteration.
- **Payments, PCI/DSS**
  We safely process your card payment(s) through the use of a secure merchant who handle the transaction between yourself and your bank, ensuring the confidentiality and security of your financial information. This also ensures PCI DSS compliance and our ability to provide fast, secure transactions to our customers.
- **Technology**
  We continually monitor our systems for possible vulnerabilities and attacks, and we carry out penetration testing to identify ways to further strengthen security. We also use hard disk encryption, firewalls, password protections, anti-virus and access checks for our employees.
  The security measures described above ensure that all reasonable steps are taken to protect your personal information.

Other divisions/brand/entities within our group

Transfers of personal data within the group are part of our business process. Activities such as filling an order, performing a credit check if needed, processing payment details, or servicing a customer request may require this sharing to take place.

We also transfer limited personal data to our vendors as required, this allows them to perform activities such as personalisation of products or direct shipping to customers.

External Organisations

In some circumstances, it may be necessary to cooperate with authorities in relevant countries in the case of fraud, regulatory or legal actions. We abide by those actions based on our legal review.

If you have provided consent to marketing information, you may also receive marketing information from external companies related to the products or services you are interested in.

We sometimes share personal data with trusted partners that provide optional services. An example of this is product and service surveys that are important to us to gather customer feedback. You are not obligated to enter any information, as they are optional.

Under no circumstances do we permit the selling of your personal data to other organisations.

International Data Transfers

In cases where we transfer data as part of our normal business activities we will have the appropriate contractual safeguards in place, including those with our suppliers.

How Long Do We Keep Your Data?

In order to provide a high-quality of service, it is necessary that we keep some data to continue to service your customer needs. As such, the following retention periods apply:

Types of data	Purpose(s)	Retention Period
Prospective Customer/Recruitment Candidate Data	For potential employment within the Mi Hub companies.	• 13 months, live 12 months, 1 month in archive.
Customer data	Execution or performance of a contract (corporate).	• Either 10 years after the last transaction takes place, or • Indefinitely if any illegal or fraud activity is detected, or it is additionally required for legal or regulatory purposes.
Telephone Recordings	To monitor customer service performance, to prevent fraud etc.	• 13 months in total. 12 months accessible, 1 month in an archive.
Accounts and legal data.	Execution or performance of a contract (corporate).	As required by UK laws. Normally 7 years.

Your Rights

When We Act as a Data Controller or as a Data Processor

If you are an employee and we have a contract with your employer, we may only be a processor of your personal data. In these cases, we forward any requests to your employer.

When we sell products through a reseller or online marketplace, again we may only be a data processor and the seller will be the actual data controller. They will respond with respect to your data rights. Any requests made though us will be forwarded to the relevant data controller and they will manage all communications with you.

If the purchase is directly through us (phone, post, website) then we are the data controller and we will respond to your request.

Under EU GDPR and UK DPA 2018 (UK GDPR), you have certain data protection rights.

- **Right to Information/Notification**
  This right provides you to ask us for information about what personal data we hold about you, how it is being processed and the reasons for that processing.

  Where you have bought a product or service from any of our resellers, or on their online stores, they will have your customer details, so any notifications or access to data will be managed by them.

  If we ever experience a data leak that could have significant negative consequences for your personal privacy rights and freedoms, then you as a customer will be personally informed of the circumstances and actions we are currently taking and will take in the future.

- **Right to Access**
  This right provides you with the ability to get access to your personal data that is being processed. You can request to see or view your own personal data, as well as to request copies of the personal data if you do not already have a copy, or you do not know it. You may also use a third party to make the request, and we will ask for authorisation proof (power of attorney etc.) if needed.

- **Right to Rectification**
  This right provides you with the ability to ask for modifications to your personal data in case you believe that the personal data is inaccurate. We are happy to do this via our customer services team or via the Data Privacy Office contact information.

- **Right to Withdraw consent**
  This right provides you with the ability to withdraw a previously given consent for processing of your personal data. The request requires us to stop the processing of that data for that specific purpose in the future. Mainly, for us, this applies to marketing activities and if you ask us to stop sending you particular or all product or services information, we will do so.

- **Right of Erasure/Right to be forgotten**
  This right allows you the ability to ask for the deletion of your data. This will generally apply to situations where we no longer have a customer relationship with you and the data has not been deleted already. In some cases, we have a legal obligation to keep certain data (invoices, financial records etc.) .and therefore this right is not an absolute right.

- **Right to Object**
  This right provides you with the ability to object to the processing of your personal data. For example; you can also ask for your data not to be processed for scientific or historical research purposes (if relevant) unless it is necessary for public interest reasons.

  However, this is also not an absolute right, as we may have legal, regulatory, contractual, or legitimate interest processing reasons to consider also.

- **Right to object to automated processing/automated decision**
  You can also object to a decision that is made automatically, and to have that decision reviewed by a person. This is usually used for credit agreements if you believe that the decision does not account for unique personal circumstances.

- **Right to Data Portability**
  If you have consented or contracted to provide us personal information and our processing is automated, then you can ask for that data to be made portable. However, at present there is no standard on which this portability occurs to allow easy transfer and we do not have partners that would use that data in this way.

Escalation to Your Supervisory Authority

In the event that you are unhappy with our processing of your personal data, you also have the right to lodge a complaint, at any time, with the relevant supervisory authority in the country where you live, or as below:

UK:	Information Commissioner's Office (ICO)	https://ico.org.uk/concerns/
NL:	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/en/contact-dutch-dpa/contact-us

If you live outside the Netherlands or the United Kingdom, your complaint will remain on file within your country, but will be addressed by one of the data authorities listed above.

Changes to this Privacy Notice

Any changes we may make to our Privacy Notice in the future will be posted on this webpage and, where appropriate, notified to you. The new terms may be displayed on-screen and you may be required to read and accept them to continue your use of our Website.