

Data Protection Policy

Contents

1. Introduction
 - 1.1 Purpose of the Policy
 - 1.2 Scope
 - 1.3 Key Principles
2. Data Collection
 - 2.1 Categories of Data Collected
 - 2.2 Methods of Data Collection
 - 2.3 Data from Third Parties
3. Legal Basis for Processing Data
 - 3.1 Consent
 - 3.2 Contractual Obligations
 - 3.3 Legal Compliance
 - 3.4 Legitimate Interest
4. Use of Personal Data
 - 4.1 Purposes for Data Use
 - 4.2 Marketing and Communications
 - 4.3 Profiling and Automated Decision-Making
5. Data Retention
 - 5.1 Data Retention Periods
 - 5.2 Criteria for Determining Retention
 - 5.3 Data Deletion and Disposal
6. Data Security
 - 6.1 Technical and Organisational Measures
 - 6.2 Data Breach Notifications
 - 6.3 Encryption and Safeguards
7. User Rights
 - 7.1 Right to Access
 - 7.2 Right to Rectification
 - 7.3 Right to Erasure
 - 7.4 Right to Restriction of Processing
 - 7.5 Right to Data Portability
 - 7.6 Right to Object
 - 7.7 Right to Withdraw Consent
8. Third-Party Sharing
 - 8.1 Data Sharing with Service Providers
 - 8.2 International Transfers
 - 8.3 Safeguarding Shared Data
9. Cookies and Tracking
 - 9.1 Use of Cookies
 - 9.2 Managing Cookie Preferences
 - 9.3 Third-Party Tracking Tools
10. Compliance with GDPR and Other Regulations
 - 10.1 Overview of GDPR Compliance
 - 10.2 Data Protection Officer (DPO) Role
 - 10.3 Reporting Obligations



11. Amendments to the Policy
12. Contact Information

1. Introduction

1.1 Purpose of the Policy

The purpose of this Data Protection Policy is to outline how Future Garments t/a Eurox collects, uses, stores, and protects personal data in compliance with relevant data protection laws, including the General Data Protection Regulation (GDPR).

1.2 Scope

This policy applies to all personal data processed by Future Garments t/a Eurox, covering employees, customers, suppliers, and any other individuals whose data we process.

1.3 Key Principles

Future Garments t/a Eurox is committed to the following key principles:

- Transparency in data collection and use.
- Adherence to legal requirements regarding data processing.
- Ensuring that data is secure, accurate, and up-to-date.

2. Data Collection

2.1 Categories of Data Collected

We collect the following categories of personal data:

- Personal identification data (e.g., name, address, phone number).
- Financial information (e.g., payment card details).
- Account login details (e.g., usernames, passwords).

2.2 Methods of Data Collection

Personal data is collected via:

- Direct interaction (e.g., completing forms on our website).
- Third parties with consent to share data with us.

2.3 Data from Third Parties

We may also collect data from third parties such as credit agencies, marketing partners, and public sources, provided that consent has been obtained.

3. Legal Basis for Processing Data

3.1 Consent

We process data when explicit consent has been provided by the individual, particularly for marketing purposes and subscription services.

3.2 Contractual Obligations

Data processing is necessary to fulfil our contractual obligations, such as processing orders and delivering products.

3.3 Legal Compliance

We may process personal data to comply with legal requirements, such as financial regulations and fraud prevention.



Aqua House, Buttress Way,
Smethwick, Birmingham, B66 3DL



Mon - Fri
8:30 am - 5:30pm



+44(0)1215557167

3.4 Legitimate Interest

Where processing is necessary for our legitimate business interests (e.g., improving services), we will ensure that these interests do not override the rights of individuals.

4. Use of Personal Data

4.1 Purposes for Data Use

We use personal data to:

- Fulfil customer orders.
- Improve and personalise our services.
- Respond to customer inquiries.

4.2 Marketing and Communications

We may use personal data for email marketing and promotional communications, subject to consent. Users can opt out at any time.

4.3 Profiling and Automated Decision-Making

Profiling may be conducted to tailor services, but users can object to this processing under GDPR.

5. Data Retention

5.1 Data Retention Periods

Data will be retained only for as long as necessary for the purposes for which it was collected, or as required by law.

5.2 Criteria for Determining Retention

Retention periods are based on legal requirements, contractual obligations, and the nature of the data collected.

5.3 Data Deletion and Disposal

Data that is no longer needed will be securely deleted or anonymised.

6. Data Security

6.1 Technical and Organisational Measures

We implement appropriate security measures to protect personal data, including encryption, secure servers, and regular audits.

6.2 Data Breach Notifications

In the event of a data breach, affected individuals will be notified in accordance with legal requirements.

6.3 Encryption and Safeguards

Sensitive data, such as payment information, is encrypted during transmission and storage to prevent unauthorised access.

7. User Rights

7.1 Right to Access

Individuals have the right to request access to their personal data and information about how it is processed.



7.2 Right to Rectification

Users can request correction of inaccurate or incomplete data.

7.3 Right to Erasure

Individuals have the right to request deletion of their data under certain conditions, such as when the data is no longer needed.

7.4 Right to Restriction of Processing

Users can request that the processing of their data be restricted under specific circumstances.

7.5 Right to Data Portability

Individuals can request that their data be transferred to another service provider in a commonly used format.

7.6 Right to Object

Users have the right to object to certain types of data processing, including direct marketing.

7.7 Right to Withdraw Consent

Users may withdraw their consent for data processing at any time.

8. Third-Party Sharing

8.1 Data Sharing with Service Providers

We may share data with trusted third-party service providers who process data on our behalf (e.g., payment processors).

8.2 International Transfers

If data is transferred outside the EU, appropriate safeguards will be put in place to protect personal data.

8.3 Safeguarding Shared Data

Third-party processors are required to comply with our data protection policies and applicable laws.

9. Cookies and Tracking

9.1 Use of Cookies

We use cookies to improve user experience and analyse website traffic. Users can manage their cookie preferences via our website.

9.2 Managing Cookie Preferences

Users can adjust their browser settings to block or manage cookies, but this may affect website functionality.

9.3 Third-Party Tracking Tools

We may use third-party analytics and advertising services that employ cookies and tracking pixels.

10. Compliance with GDPR and Other Regulations

10.1 Overview of GDPR Compliance

We comply with GDPR and other data protection laws to ensure that personal data is processed lawfully, fairly, and transparently.

10.2 Data Protection Officer (DPO) Role

We have appointed Hardip Palak as our Data Protection Officer responsible for overseeing compliance with GDPR.



10.3 Reporting Obligations

We comply with regulatory reporting obligations related to data protection and cooperate with relevant authorities when required.

11. Amendments to the Policy

We may update this policy from time to time to reflect changes in our practices or legal requirements. Any significant changes will be communicated to users in a timely manner.

12. Contact Information

For any questions or concerns regarding this policy or the handling of personal data, please contact our Data Protection Officer at:

Email: [Hardip.Palak@future-gmts.com]

Address: [Aqua House, Buttress Way, Smethwick, West Midlands, B66 3DL]

Signed:



Kuldip Palak
Managing Director
Date:31/07/24

Signed:



Hardip Palak
Commercial Director
Date:31/07/24



Aqua House, Buttress Way,
Smethwick, Birmingham, B66 3DL



Mon - Fri
8:30 am - 5:30pm



+44(0)1215557167