



General Data Protection Regulation

GDPR Policy

Issue: **A3/250126**

Company: **Andrews Fasteners Limited**

Policy apply from: **25/05/2018** (no request for data before that date will be processed)

Last Review: **25/01/2026**

The company recognises **UK's data protection legislation** (UK General Data Protection Regulation and the Data Protection Act 2018), and based on its requirements draw below **GDPR Policy**.

➤ *Additionally, to this document, company operate internal Data Protection Policy (QCD 190).*

The company, to carry out activities necessary to maintain its business, on a daily basis shall be collecting a variety of data, including personal data. This data is processed through necessary activities within the company and outside the company but remaining under the company control.

As our company is mainly oriented for business customers, we are processing only a limited amount of **Personal Data** in relation to Orders and Enquiries from private customers. The data is processed only for business enquiries and when finished, none of this data is reused without consent with an exclusion when asking for a Feedback in relation to the order.

We are taking an extensive duty of care to assess and monitor the security of the equipment, services and our website to ensure, that the data that we process are secure.

For the latest version of GDPR Policy please follow our website:

<https://www.andrewsfasteners.uk/gdpr>

GDPR Policy - Content

1. Breach notification

If the company shall experience any identified data breach to its equipment (server, company computers, file storage, processing equipment), services (email, cloud file exchange) or website, appropriate users will be notified without undue delay **when the personal data breach is likely to result in a high risk** to their rights and freedoms.

The company will notify the **supervisory authority (the Commissioner) without undue delay** and, where feasible, **not later than 72 hours** after becoming aware of a breach, unless it is unlikely to result in a risk to individuals (**unlikely to result in a risk to the rights and freedoms of natural persons**).

The company has in place necessary precaution measures to prevent data breach (i.e. Backups, Firewalls, Antivirus software, Strong Passwords, Encryptions of data etc.). These measures are subject to the test of its security on a routine basis.

2. Data collection, processing and storage

a. Right to Access

Users have the right to check with the company what data point is/has been collected, where are the data points processed and stored, the reason behind the collection, processing and storage of the data. Users have the right to update the data, and where the consent has been



General Data Protection Regulation

GDPR Policy

Issue: **A3/250126**

given to process it (i.e. for marketing purposes), have the right to withdraw the consent for that use.

Following a user request, the company intends to respond **without undue delay and in any event within one month of receipt.**

The data will be provided **free-of-charge** unless it falls into specific criteria, where an administration charge will apply (if the request is **manifestly unfounded or excessive**).

Data will be provided in electronic form free of charge.

Any charges will incur 20% VAT, proforma payment to be made prior to order processing.

b. Right to be forgotten

The user has the right to be forgotten and can express their decision to erase any personal data and stop its further collection and processing at any point.

In addition to the requirements from GDPR, the company is also complying with other International and Local Standards and Regulation (Health and Safety, Quality Management Systems). In such cases, when a user will require removing its data, and this data is necessary to be held in the archive, for example, for a minimum of 10 years, the company reserves the right to refuse but will then advise the user the earliest date when this can happen.

Please be advised, that due to International Standards requirements and National laws (laws that we are legally obligated), there is a requirement for keeping personal records in the file for the period of time that varies from 6 months to even 10 years from last time the data has been used (NHSS3 – National Highway Sector Scheme 3). The company expressed the right to refuse to erase any personal data that it is legally obligated to keep. However, the company agreed to stop further collection and processing of user data following his request.

c. Data Portability

The right to data portability applies if the processing is based on **consent** OR if it is necessary for the **performance of a contract**.

Any content of contact forms used on the company website is directly forwarded to company email address instead of storing them on the server side. The company reserves the right to store the data on the server side for short period of time, on which user will be advised if that's the case during their request for data.

3. Accessibility to data

User data will be provided via e-mail or through cloud storage (in case of extending of data) free of charge and will be available for access for a period of one month following the date when we're prepared. Any other form of providing data can be considered but will be subject to administration charge as specified in 2.a above.



General Data Protection Regulation

GDPR Policy

Issue: A3/250126

The company reserve the right to verify the person who requests their data (**only where they have "reasonable doubts"** concerning the identity of the person) by asking to confirm recently obtained data with that person. Failure to verify the validity of their data may result in a refusal to act on the request. For verification, the company may ask to provide a copy of identification document that will be used through the request and destroyed one month after the decision in relation to the request.

When following a user request, the company will manifestly unfound any data will:

- a. Refuse to act on the request
 - i. The user has the right to request from the company to demonstrate the manifestly unfounded data.
 - ii. Following the request to demonstrate the manifestly unfounded data an **reasonable fee based on administrative costs** will apply and need to be paid together with the request.
 - iii. In case of refusal, the user has the right to complaint to the supervisory authority and to a judicial remedy.

4. How the company is collecting it data

- a. Hard Copies (Enquiries, Drawings, Acknowledgments, User Data)
- b. Software (Applications, Scans, databases)
- c. Services, i.e.
 - i. E-mails
- d. Website and web-services i.e.
 - i. Google Analytics
 - ii. Content Delivery Network (CDN)
 - iii. Contact forms, Comment forms, Newsletters signups etc.
 - iv. Web Chats
- e. Social Network

And other methods of data collection necessary to serve its business to customer.

During data collection, the company will use various technologies, where each one refers to their own GDPR policy. If you require to access data gathered by a third-party, that our company is not able to access, you need to contact them directly.

5. How to request your data?

To request your data, please

- a. send an email to gdpr@andrewsfasteners.uk, or
- b. via post:

Andrews Fasteners Limited

Unit 8, Latchmore Park, Latchmore Road, Leeds, LS12 6DN, West Yorkshire, United Kingdom

- c. via the website:

<https://andrewsfasteners.uk/gdpr/request>



General Data Protection Regulation

GDPR Policy

Issue: **A3/250126**

On your request, you need to provide us with information's allowing us to identify correct data for correct use without confusions. In case of misinformation the company reserve the right to postpone data request until full details are received.

To process your request, we require sufficient information to identify you within our records; this may include **Name** and **Surname**, **Residence address**, **e-mail address**, contact **phone number**. Providing any additional information allowing us to swiftly process your request will be appreciated. Any data gathered during this request will be removed within one month after the request has been finished unless it is required by appropriate law or regulation to hold for a longer period of time.

Data subject requests **may be provided orally**, provided identity of the requested is proven.

Following your request, if the company **deems a request unfounded or excessive**, it will **notify the user of the fee** before proceeding.

Payment is processed online through <https://afast.uk/pay> and operated by Square.