MARSDEN

GDPR

Compliance Policy

Guidance for employees

v.1.1 February 2024

Contents

What is GDPR?

The **Data Protection Act 2018** is a regulation in UK law and is the implementation of General Data Protection Regulation (GDPR) for all individuals within the European Union.

The regulation basically covers:

1. The data we hold on individuals and companies
2. What we do with that data

GDPR and the Data Protection Act 2018 replaces the Data Protection Act 1998.

From 25th May, 2018, any company found to be in breach of GDPR will be subject to a fine of up to €20 million or 4% of turnover - whichever is higher.

The principles of GDPR

The regulations require that personal data shall be:

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

It also requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Why does this policy document exist?

This data protection policy ensures Marsden Weighing Machine Group:

1. Complies with GDPR and follows good practice
2. Protects the rights of staff, customers and partners
3. Is open about how it stores and processes individuals' data
4. Protects itself from the risks of a data breach

It is intended as a guide for employees and to ensure Marsden is GDPR compliant. It can be used as a reference document for anyone needing to understand how and why Marsden complies with GDPR.

Responsibilities

Everyone who works for Marsden Weighing Machine Group has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

1. **Chief Financial Officer** is responsible for:
    - Keeping the board updated about data protection/GDPR responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule
    - Arranging, where necessary, appropriate training and advice for the people covered by this policy
    - Handling data protection questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data Marsden Weighing Machine Group holds about them (also called 'subject access requests')
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

2. IT consultant **IT-F1** is responsible for:
    - Ensuring all systems, services and equipment used for storing data (non-website) meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

3. Web consultant **Evoluted** are responsible for:
    - Ensuring all systems, services and equipment used for storing data (relating to, and including, the company website/s) meet acceptable security standards

- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data.

4. The **Marketing Manager,** is responsible for:

- Approving any data protection statements attached to company communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Management and segmentation of in-house data lists
- Management and use of purchased data lists

Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

1. The only people able to access data covered by this policy should be those who **need it for their work**.
2. Data **should not be shared informally**.
3. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
4. In particular, **strong passwords must be used** and they should never be shared.
5. Personal and company confidential data **should not be disclosed** to unauthorised people, either within the company or externally.
6. Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees **should request help** from their line manager if they are unsure about any aspects of GDPR or handling data.

What is personal data?

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data can be anonymised (removing elements of the data so that the data subject(s) cannot be clearly identified) or pseudonymised (key coded so that access to another document, or a password, is required to identify the data subject(s).

Personal data stored by Marsden Weighing Machine Group must be protected so that data subjects cannot be identified.

For example: the Website Orders Google doc originally contained the following data relating to the customer:

Order number
Website order number
Order type
Date received
Product code
Quantity
Price
Customer name
Customer email address
Customer phone number
Customer postcode
Customer Account Code
Industry

In order to anonymise the data, customer email address, phone number and postcode have all since been removed meaning a data subject cannot be easily identified without having access to the company CRM or Sage.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to **the Chief Financial Officer**.

Data stored on paper should be avoided. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

1. When not required, the paper or files should be kept in a locked drawer or filing cabinet.
2. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
3. Data printouts should be shredded and disposed of securely when no longer required.
4. Marsden operates a clear desk policy. At the end of the working day, every desk should be clear of any paperwork that may be deemed sensitive/confidential. Every employee is responsible for their own desk.

Please note that data relating to consumer or sole trader customers must not be stored unless it is for accounting/billing purposes (i.e Sage).

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

1. Data should be protected by strong passwords that are changed regularly and never shared between employees.
2. If data is stored on removable media, like a USB, these should be kept locked away securely when not being used.
3. Data should only be stored on the company CRM and Sage, or in exceptional circumstances where there is adequate security and protection, in a spreadsheet. However, this must only be for analytical purposes or for uses that are in the customer/company interest. External, encrypted cloud based storage systems may be used, but only those agreed by **the Chief Financial Officer**.
4. Data may be saved away from the company CRM or Sage only if it has been pseudonymised or anonymised (see page 9).
5. Servers containing personal data should be sited in a secure location.

6. Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
7. Personal and company confidential data should never be saved directly to laptops or other mobile devices like tablets or smartphones. Always use well-protected cloud based storage systems (see note 3), the company's shared Common drive or CRM/Sage.
8. All servers and computers (and website) containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Marsden Weighing Machine Group unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

1. When working with personal data, employees should ensure the screens of their computers are always locked when left unattended. Auto lock should be set at 1 minute or less (see also Page 24, Use of mobile phones/tablets/laptops).
2. Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
3. Data must be encrypted before being transferred electronically. The Operations Manager can explain how to send data to authorised external contacts.
4. Personal data should never be transferred outside of the EU.
5. Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Direct Marketing

Under GDPR, the most important concern with Direct Marketing is consent. The recipient must be opted in to direct marketing for Marsden Weighing Machine Group to have permission to direct market to them.

Direct marketing encompasses:

Email/email campaigns
Sales/marketing phone calls
Communication regarding a quotation (sending the quotation, following up the quotation)
Marketing via post
Sales/marketing text messages

It is important to determine whether a customer is a business, a sole trader or a consumer. A business is ‘opt out’ (they can be direct marketed to but have to ‘opt out’ for this to stop). Sole traders and consumers are ‘opt in’ (we have to have permission from them - i.e they must opt in - before we can market to them).

Marsden Weighing Machine Group is taking a blanket policy that sole traders and consumers will not be direct marketed to at all. We will continue to direct market to businesses unless they have opted out.

More information on how contacts may be contacted if they are opted in can be found under **How we contact those who have opted in**.

Sole traders and consumers must not be included in the following:

1. Email campaigns
2. Quotation chasing (we can send a requested quotation, but since chasing a quotation is regarded as direct marketing, we cannot communicate further unless requested to do so)
3. Sales/marketing phone calls

Marsden does not send marketing via text or post (except for medical catalogues, which are sent to NHS contacts/dealers only).

Data roadmap

It is important to understand the way data is processed within Marsden Weighing Machine Group. This should ensure that data is handled correctly and in the interests of the customer and Marsden Weighing Machine Group.

1. Sales through the website

Sales directly through the Marsden Weighing Machine Group website are stored within the Sales area of the Admin Panel. Only **the Marketing Manager and Evoluted** have access to this.

(nb: when entering billing/shipping details, the customer is given the following information for each field):

Billing information

First name
Your name will be added to the order/billing documents

Last name
Your name will be added to the order/billing documents

Company
Your company's name will be added to the order/billing documents

Email address
We will send order documentation via email

Address
The address you add here will need to match the address you card is registered to for your payment to be processed

City
The address you add here will need to match the address you card is registered to for your payment to be processed

Postal Code
The postcode you add here will need to match the address you card is registered to for your payment to be processed

Country
The country you add here will need to match the address you card is registered to for your payment to be processed

Telephone
We will only contact you by telephone if there are any issues with your order

Shipping information

First name
Your name will be added to the shipment

Last name
Your name will be added to the shipment

Company
Your company's name will be added to the shipment

Address
Please add the address here that you wish your order to be delivered to

City
Please add the address here that you wish your order to be delivered to

Postal Code
Please add the postcode here that you wish your order to be delivered to

Country
The country you add here will be added to the consignment details

Telephone
If the shipping address is different to the billing address, you may want to add a phone number here in case there are any delivery issues)

An email of the order details is generated and sent to sales@marsdengroup.co.uk, along with a payment confirmation from the bank (payment itself is handled by the bank and not Marsden Weighing Machine Group). The payment confirmation email from the bank also includes the customer's name, address and order value.

(Note: Emails to and from sales@marsengroup.co.uk are accessible by multiple staff members and multiple devices, therefore greater care should be taken when using this method of communication and information sharing. Do not forward or reply to emails containing personal or company confidential data without remove/anonymising information first.)

The customer's details/order details are entered into the company's CRM system which is then synced with Sage. Consumers and sole traders are marked as not to contact in the CRM system.

The contact at the business is set to 'yes' for opt in when their details are entered as an Organisation.

When opt in is 'yes' the contact will be included in relevant email marketing campaigns, unless they choose to opt out. The contact can opt out at any time by phone, via the unsubscribe link on an email campaign or via email. They will then need to be set to 'no' and free text box used to record how (and why, if known).

The order, with customer name, address, order details and any other contact information provided, is transferred electronically along with the payment confirmation email on the CRM system. The order confirmation is sent to the factory for product preparation and despatch.

More information on how contacts may be contacted if they are opted in can be found under **How we contact those who have opted in**.

2. Sales over the phone

When a customer orders over the phone, the details of the order and the customer are recorded on a Customer Order Form ('green sheet'). Payment information is entered directly into the banking site online.

The customer’s details/order details are entered into the company’s CRM system which is then synced with Sage. The customer order form is saved on the CRM system electronically.

The contact at the business is set to ‘yes’ for opt in when their details are entered as an Organisation, as in 1.

The order, with customer name, address, order details and any other contact information provided, is stored on the CRM system along with the payment confirmation email. The order confirmation is sent to the factory for product preparation and despatch.

More information on how contacts may be contacted if they are opted in can be found under **How we contact those who have opted in**.

3. Orders via email

Marsden will often receive email orders. The customer may either be proforma or have an account.

The customer’s details/order details are entered into the company’s CRM system which is then synced with Sage. The customer order and email is saved on the CRM system electronically.

Business contacts will be opted in unless they ask to be opted out; consumer/sole trader information will be marked as do not contact on the CRM system.

The order, with customer name, address, order details and any other contact information provided, is stored electronically on the CRM system. The order confirmation is sent to the factory for product preparation and despatch.

More information on how contacts may be contacted if they are opted in can be found under **How we contact those who have opted in**.

Contact Forms

General enquiries via:

https://www.marsden-weighing.co.uk/index.php/contact/
https://www.marsden-weighing.co.uk/index.php/bespoke-weighing-scales/
https://www.marsden-weighing.co.uk/index.php/services/

...can be responded to in relation to the enquiry only. There is no request for permission to respond to the query since there is a legitimate interest that covers Marsden Weighing Machine Group in a relevant response to the enquiry.

Customers can enter either their phone number or email address, or both. There is no requirement for them to enter both and must be contacted via the method they have provided if only one form of contact has been entered.

Enquiries should be marked as ‘opt out’ unless/until the contact becomes a customer, at which point they can be opted in at the point that the order is processed and the CRM updated.

This process applies also to enquiries via email, phone and Chat.

Enquiries: General note

Enquiries via any channel are entered into the CRM if notes on the enquiry need to be made or a quotation needs to be raised. If there is no business benefit, or benefit to the enquirer, they must not be recorded in the CRM.

Emails containing customer data

One of the least secure methods of accessing/sharing customer information is via email. This is because:

- Recipient email addresses can be incorrectly entered meaning the wrong person receives customer data
- The device (tablet, smartphone, PC etc) of the recipient may not be secure
- Emails - particularly to external recipients - may be intercepted

Sending customer data or company confidential information via email, either internally to colleagues or externally, should be avoided, and instead sensitive data, documents and messages should be saved to the Common Drive and that location shared with the recipient. When scanning sensitive documents, always save to the Scans folder and never scan to email.

Customer data should be treated in the same way as credit card details and, if a customer’s details or order do need to be emailed, only essential information included.

Emails containing employee data

Sending Employee data or confidential information via email, either internally to colleagues or externally, should be avoided, and instead sensitive data, documents and messages should be provided in hard copy format directly to the responsible individual who will then save it to the HR Drive or BrightHR. When scanning sensitive documents, always save to the Scans folder and never scan to email.

Some examples of personal and sensitive employee data that should be avoided being sent via email are:

- Employee's change of address
- Sickness notes
- Return to Work documents

Personal and sensitive employee data should only be emailed to Indy Purewal, Emma Lowrie or Sam Featherstone who have 2 Factor Authorisation on all email access and will then be stored on a secure server or BrightHR.

Access to the HR Drive is limited to Indy Purewal, Emma Lowrie and Sam Featherstone. Access to employee data on BrightHR is limited to Indy Purewal, Emma Lowrie, Sam Featherstone and the individuals line manager.

Please speak to the Chief Financial Officer with regards any HR/Finance issues or questions.

Management and use of purchased/leased data

Marsden is committed to ensuring the protection and privacy of individuals' personal data in accordance with the General Data Protection Regulation (GDPR). This statement outlines our approach to management and use of purchased data and our commitment to compliance with GDPR principals.

1) Data ownership and responsibilities

Marsden works closely with a number of reputable suppliers to source GDPR compliant data which has been ethically obtained. This data will then be used to contact customers with targeted messages, in alignment with the usage rights of the data.

2) Lawful basis for processing

We ensure that all data processing activities involving purchased/leased data are conducted on lawful grounds as defined by GDPR. This includes obtaining consent from individuals or replying on other legitimate grounds for processing.

3) Purpose limitation

Data purchased/leased by Marsden is used only for the specific purposes for which it was acquired. We do not engage in any processing that goes beyond the scope outlined at the time of purchase.

4) Data accuracy and quality

We take responsible steps to ensure that the data purchased is accurate and up to date. Periodic reviews and updates are conducted by the data supplier to maintain the quality and relevance of the information.

5) Security measures

Marsden employs robust security measures to protect the purchases data from unauthorized access, disclosure and data breaches. We regularly assess and enhance our security protocols to mitigate risk.

6) Data subject rights

Individuals whose data we process have the right to access, rectify, erase or restrict the processing of their personal information. Marsden will also be transparent in disclosing the nature in which it obtained the individuals data if requested. Marsden respects and facilitates the exercise of these rights in compliance with GDPR.

7) Data sharing and third parties

Marsden does not share or sell data with third-party companies.

8) Data retention

Purchased/leased data is retained only for as long as the contact duration with our supplier. Once the data leasing period has lapsed, data is securely and permanently deleted.

Opt in/opt out process

It is Marsden Weighing Machine Group company policy to auto opt in new business customers, and auto opt out all consumer and sole trader data. Direct marketing will never be sent to sole traders or consumers.

If it is not possible to determine whether the subject is a sole trader/consumer or business, they should be automatically opted out.

Please note that if a customer is to be contacted and you are unsure whether you have the necessary permission, check the Opt in status first, followed by the method field, and finally, if you are still unsure, speak to **the Marketing Manager**.

Opt in policy

Auto opt-in for businesses applies to those that have become customers.

However, enquiries that are entered into the CRM can be opted in. They will not be included in email campaigns to customers as long as the ‘Opt out’ checkbox on the contact record is set to ‘no.’ If you are unsure for any reason, always use caution and opt them out.

Examples of reasons to give alongside ‘Yes’ for opt in include:

- Business customer product enquiry
- Requested to be added to mailing list
- Became business customer
- Expressed interest in other products which made opting them in valid

At 25/05/2018, all existing customers, unless previously opted out, were set to ‘Yes’ under opt in.

Opt in process

A business customer can request to opt out in any way they wish. The process is:

- Via email campaign: A customer can opt out by clicking the ‘Unsubscribe’ button. This will automatically opt them out on the Marketing system, changing their opt in status to ‘No.’ The free text box will be auto populated with ‘Email response to

mailer’ and the update date/timestamped. The customer will be excluded from all future email campaigns, and their opt out must be observed and considered when they need to be contacted for any reason in the future.

- Via email/contact form: A customer may want to opt out via contact form or email. If this is the case, ensuring that they provide adequate information at this stage, they must be set to ‘No’ as their Opt in status. The email can also be included under Notes if this is deemed suitable.
- Via telephone: A customer may call to opt out. If this is the case, ensuring that they provide adequate information at this stage, they must be set to ‘No’ as their Opt in status.

All consumers and sole traders will be automatically opted out, and their details only stored on the CRM if it is in the interests of Marsden Weighing Machine Group or the customer (e.g a quotation needs to be kept, there is a correspondence trail that needs to be recorded on the CRM.

Following up quotations

Since Marsden Weighing Machine Group does not conduct telemarketing campaigns, opt in recording has not been granulated on the CRM.

However, following up a quotation is regarded as direct marketing, care must be taken when calling a customer to check the status of a quotation.

1. Quotation follow up process

In order to ensure that a customer is not ‘hounded’, quotation follow up is done so at a reasonable frequency and to ensure Marsden Weighing Group understands the needs and situation of the customer, and to give the customer adequate warning prior to a quotation expiring.

Enquiries under £1000:
Quotations chased after 7 days from date of quotation, then after 21, 50, 90 and 150 days.

Enquiries over £1000:
Quotations chased after 3 days from date of quotation, then after 10, 21, 50, 90 and 150 days.

Quotation then closed off on the CRM as ‘no sale’ at the same time as the final follow up.

Use of mobile phones/tablets/laptops

Marsden Weighing Machine Group’s policy is that all mobile phones or tablet devices (including service engineer tablets) that have access to company email or systems must be adequately protected with a strong passcode.

Work emails should only be accessed on mobile phones or tablet devices via the official Outlook app, and not the default iOS/email app.

Laptops that have such access will need to be protected with a strong password and must be logged out of when the laptop is not in use or left unattended.

All devices must be set to self lock at 1 minute (or sooner).

Work devices must only be used by the employee to which they have been assigned.

If a mobile phone, tablet or laptop is lost or breached, the employee must notify Emma Lowrie immediately.

Requests for personal information

Under GDPR, individuals have a right to access their personal data. This is usually referred to as ‘subject access.’

An individual may request this via email, and once such a request is received Marsden Weighing Machine Group has one month to respond. We cannot charge for this service.

Please forward all requests for information to **the Chief Financial Officer**. If you have any doubts about the identity of the person making the request you can ask for more information. Only information essential to meeting their request must be asked for, however.

If data is requested by a third party, you must be satisfied that the third party is acting on behalf of the individual.

Useful links and information

Our Privacy Policy can be found on our website here:

https://www.marsden-weighing.co.uk/index.php/privacy-policy-cookie-restriction-mode/

ICO Registration reference: ZA381192

GDPR documents: Common/GDPR General Data Protection Regulation