fwd FEDERATION OF WHOLESALE DISTRIBUTORS

WHOLESALERS GUIDE TO GDPR

THE LAW ON DATA PROTECTION IS CHANGING

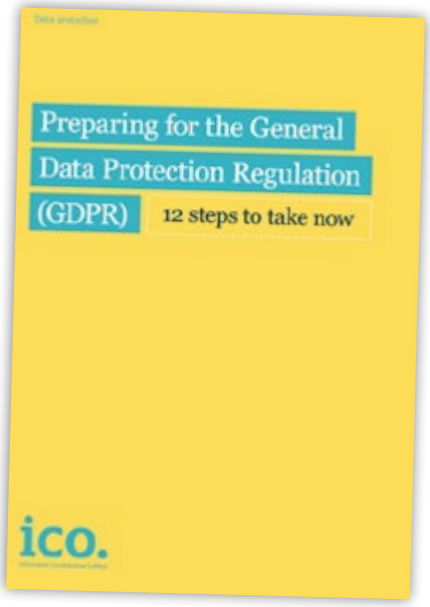
From May 25 2018 wholesalers will have to comply with new data protection laws set out in the General Data Protection Regulation, known as GDPR.

This means you will have to look at the **personal data** you keep on your customers, how its collected, how it's stored and how you share it. It may affect your mail, emails, texts and phone calls to your customers.

You need to think about the **promotional leaflets, price lists, new product notifications, invites to trade days, even birthday cards you send to your customers**, and make sure you are using their personal data within the new laws.

The **good news** is, if you're already complying with current data protection rules, you're already well prepared for adopting the new regulations.

The **bad news** is, if you don't make the necessary changes by May 25, you could be hit with an eye-watering financial penalty. The fines for non-compliance will be severe.



We recommend you read the ICO 12 step guide to preparing for GDPR

WHAT YOU WILL NEED TO DO

You will need to review the personal data you record and how you use it.

You will need to keep a record of the data you hold, including where it came from and how you use it.

You will need to be able to provide your customers or your employees with any personal information you hold on them, free of charge, within one month of them asking for it.

If someone asks you to delete their data, you must do so, unless there is a good reason for keeping it.

You will have a duty to keep this information secure, and to report any data breach to the Information Commissioner's Office

You will need to explain your lawful basis for holding the data.

You also have to make it clear that individuals have a right to complain to the Information Commissioner's Office if they think there is a problem with the way you are handling their data.

GOING PUBLIC ABOUT PRIVACY

You have to publish a privacy notice, which lets your customer know they have these rights, in a way that is easy to understand, not buried in legal language and small print.

The privacy notice must include:

- What personal data you collect
- Why you collect it and how it is used
- Who it will be shared with
- When and why it will be deleted
- What you will not use personal data for
- Your reason for keeping somone's data
- Here's an example of a Privacy Policy

THIS IS THE BIG ONE:

Your customers must actively agree to receive marketing messages from you. This includes leaflets, emails and texts. They have to choose to receive them ('opt in') rather than tell you not to send them ('opt out').

Don't panic! You may not need to get new consent from customers on your existing mailing lists to send out marketing messages. Read on...

Consent

The best lawful basis for processing personal data, from the wholesaler's point to view, is consent. You should consider sending a consent form to all your customers **NOW** and getting them to opt in to receive marketing messages from you after May 25.

Your consent form should ask them to update their contact details and give them choices on how you contact them – by telephone, email, post or SMS, or any combination of these. They must also have the option to opt out completely. You should include your privacy note (see above) with this form.

Legitimate Interest

If getting consent is not practical there's another 'lawful basis' called legitimate interest. This means you can use someone's personal information to contact them if it's a legitimate part of your business, which includes commercial interests. This could be the 'lawful basis' that justifies using your customers' data, but be careful – it has limitations.

From the ICO's guide to GDPR: Legitimate Interests

- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test.
    - Purpose test: are you pursuing a legitimate interest?
    - Necessity test: is the processing necessary for that purpose?
    - Balancing test: do the individual's interests override the legitimate interest?
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect you to use their data in a certain way, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy policy

GDPR specifically mentions marketing as a potential legitimate interest, but you must be able to show that the way you use people's data is proportionate, has a minimal privacy impact, and that people would not be surprised or likely to object. For electronic communications, you also need to be aware of the Privacy and Electronic Communications Regulations.

Other legal basis

You can also store and use someone's personal information if it's to fulfil a contract, if there's a legal obligation, or if it's in their vital interests.

It's not enough to comply...

...you have to be able to demonstrate that you comply too. You are expected to implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

BEFORE MAY 25 : OUR ADVICE TO WHOLESALERS

1 Carry out an **information audit**. Set out clearly and in detail:

- The type of personal information you hold (both computer and paper records) on your customers and staff.
- Who gave you the information or where you got it from.
- If you have clear permission to use the information, for example to send regular marketing messages.
- Who you share the information with.

2 Identify your legal basis for holding and using this data. If it is consent, you will need records that show all your customers have opted in.

3 If your legal basis is legitimate interest, you must be able to explain this basis for using data, and make that public.

4 Update your privacy policy to include the new measures required under GDPR.

5 Make sure you have procedures for:

- Deleting data if asked to
- Making someone's data available to them
- Preventing and reporting data breaches
- Carrying out Data Protection Impact Assessments

6 You may wish to appoint a Data Protection Officer to look after GDPR compliance. In some cases this is a legal requirement – in others it's just good practice.