

New data protection regulations come into force across the UK on May 25 2018. This will impact how you interact with your customers and the general public and how you handle personal data. The Association has released a comprehensive document on the GDPR which all business owners should be familiar with. This document is designed to assist store staff in the major changes that will impact them.

1. *Privacy Notice to be made available before collecting data*

Before a staff member collects any personal data from potential or existing customers they must be offered a copy of the business's privacy statement. This would apply before filling out a contract or taking details to follow up a quote with the person. If the person is in store, then you should have a printed copy of the privacy notice available for them to view or take away. If the enquiry is online, then there should be a link to the privacy notice before they enter their data. You should be familiar with the contents of the privacy notice so that you can answer any questions.

2. *Consent boxes must be completed by the customer*

Your new storage agreement probably has at least one box that the customer is required to tick in order to provide consent for marketing or further contact. The customer must tick this box freely of their own accord. If you pre-fill contracts for customers then you cannot tick this box and must have the customer tick it when signing the agreement. You can not insist they sign it in order to receive storage. You can however explain the importance of signing it to allow the business to communicate relevant offers and information to them.

3. *Know who in the business is responsible for data protection*

While your business may not have a formal data protection officer it will have someone who is primarily responsible for data protection, reporting breaches, removing data and the like. You should know who this person is so that you can communicate issues with them if required and also refer customers to them if required.

4. *Know what to do if anyone asks you for copies of their data, to remove consent or alter a person's data*

People have certain rights to get copies of or amend or remove their data or revoke their consent at any time. You should know what the procedure is for handling these requests within your business. There is a strict time limit for compliance with such requests, so it is important you act promptly.

5. *Understand your legal basis for collecting data*

Customers may ask you the legal basis you have to collect their data. This is detailed in your privacy notice, but you should be aware of the situations when each method applies. Generally the "contractual purposes" basis will apply for all routine customer account administration and correspondence with existing customers. "Legitimate business interests" will apply when you follow up on enquiries from customer prospects, however if you intend to direct market to people, give the data to 3rd parties for marketing or market to the customer after they have stopped storing with you then this will most likely require consent. You will need to know what the procedure is within your business for obtaining consent.

6. *Know how to keep data safe*

You need to make sure you do everything you can to keep personal data safe. You should know what the best practice requirements are within your business to prevent unauthorised access to personal data. This will include basic cyber security measures for how you use the business's IT systems and how you keep paper records safe.