01 March 2018

scottish licensed trade news

Are you ready for data changes?

With laws on data management changing it's vital hospitality firms are compliant, writes Laura Irvine of BTO Solicitors

Laura Irvine

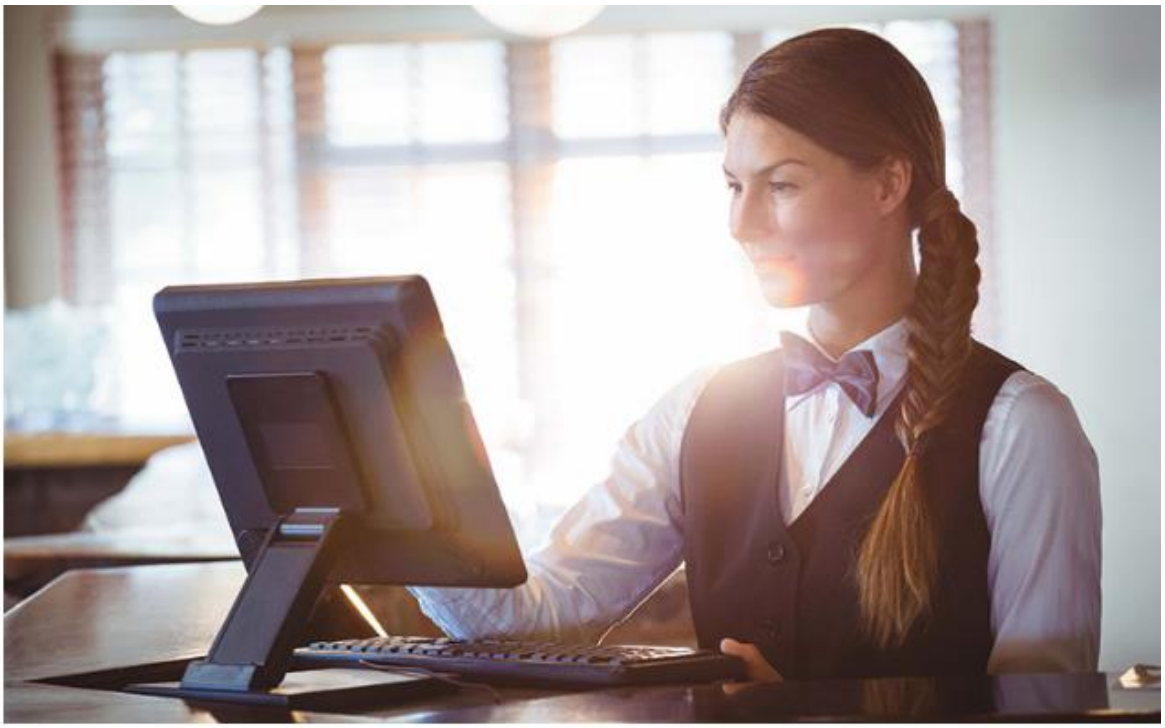
THE General Data Protection Regulation (GDPR) comes into force on May 25, 2018 and will change the way organisations within the EU process personal data.

The GDPR will be supplemented by a new UK Data Protection Act (DPA) and will increase the obligations on all organisations using or processing personal data.

The new regulations are particularly pertinent for businesses in the hospitality sector, with large banks of sensitive customer data as well as mailing lists for marketing purposes.

It will become much more difficult to obtain valid consent under the GDPR, but there are other lawful bases which have been ignored under the DPA.

It is not always about consent. An organisation must identify what lawful basis it is relying on: is it necessary for you to gather the data to provide a service or to comply with a contract of employment? Any processing must also be done in a transparent manner, which means telling employees and customers what you are doing with their data, even if you do not require their consent.



The rules governing the handling of personal data are changing at both a European and British level.

Under the GDPR you must provide information about processing in a Privacy Notice at the time you collect it.

This includes your legal basis for processing; whether the data is passed to other organisations and how long you will keep their data. You must also tell them about their rights in relation to their data including the right to complain to the Information Commissioner's Office (ICO).

There are some enhanced and some new rights.

For example, an individual can ask for a copy of their personal data and you must comply within 30 days. In certain circumstances, there is a right to be forgotten; a right to restrict processing and a right to object to processing.

Most organisations require to keep a record of processing – it is obligatory if you have 250 employees or more, but smaller organisations must also record any high risk processing ie. processing of health data or criminal offence data. It is essential that organisations understand what data they are processing to ensure compliance.

Both types of organisation have obligations to comply with the law and both can be investigated and fined. If you are passing data to a third party who acts on your instructions in relation to storage or destruction of personal data, etc. then you must have a written contract in place which sets out strict terms to ensure this is all done in compliance with the GDPR.

A personal data breach must be reported to ICO without undue delay and within 72 hours of it being discovered unless there is likely to be no risk to the privacy rights of any individual. If there is a high risk to the privacy rights of individuals, then they must also be notified without delay.

The ICO will have the power to impose fines up to a maximum of €20 million or 4% of global turnover, whichever is higher, for processing breaches (not just personal data breaches), and €10 million or 2% of global turnover for administrative breaches.

If your organisation is sending marketing emails or SMS messages, you must work out whether you are relying on consent. If you are, then you must ensure that you can demonstrate that consent complies with the new standards under the GDPR.

Consent must be freely given and an unambiguous indication of the individual's wishes.

Pre-ticked consent boxes are a thing of the past.

• Laura Irvine is a partner at BTO Solicitors.