HEWITSONS

GDPR & RURAL BUSINESS

The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018. It is an EU Regulation but it is intended that the Data Protection Bill (which may ultimately become the Data Protection Act 2018) will be enacted to ensure that the GDPR remains with us post-Brexit.

Although many requirements under the GDPR are similar to those which currently exist under the Data Protection Act (DPA), the GDPR does impose additional obligations and creates potential liabilities.

The GDPR applies to all businesses (and also other organisations or individuals) that hold or process personal data. "Personal Data" is any information through which a person can be identified, either directly or indirectly. So if you hold data and you can see that it relates to an identifiable person it is caught by the GDPR. This could include customer lists for the farm shop, marketing lists for venue hires, names and addresses of contractors you use, details of your tenants etc.

The GDPR is an "outcome based" regulation meaning there is not a single set of rules that you have to tick off, but instead businesses need to demonstrate they comply with certain principles.

Accountability

Businesses will need to ensure that personal data is processed in accordance with principles of:

- Lawfulness, fairness and transparency. For example the person must know who is collecting their data, why it is being collected and who it may be shared with. Personal data can only be collected for a specific and justifiable reason.
- Purpose Limitation and Data Minimisation. The personal data must only be collected for specific limited purposes. The data collected must be adequate for that purpose but not be excessive.
- Accuracy. Reasonable steps must be taken to ensure personal data collected is and remains accurate.
- Storage Limitation. Personal data should not be kept for any longer than reasonably required, bearing in mind the purpose for which is was collected.
- Integrity and Confidentiality. Reasonable steps should be taken to ensure the data is kept secure and confidential. For example ensure software and all security policies are up to date, you have appropriate hardware and virus protection software.

- For businesses where employees handle the personal data you should introduce appropriate organisational measures such as staff training, internal audits of processing activities, and reviews of HR and privacy policies. Businesses should have policies in place to ensure compliance with the above principles and ensure staff are aware of and follow the policies.

- Businesses with more than 250 employees or which process personal data more than occasionally (or in certain other circumstances), must maintain written records of processing activities. There will be relatively few farming or Estate businesses with 250 or more employees. However this may catch an Estate Office which routinely processes tenants' data.

If your business collects that personal data, and determines the purposes and the means of the processing (meaning you are the "Data Controller") but passes it to a third party processor (a "Data Processor") you need to take reasonable steps to ensure the Data Processor complies with the GDPR principles. For example if you collect the data of tenants but the portfolio is managed by a firm of agents, the agents would be Data Processors. You should ensure that the terms of your agreement with your agent are sufficient and require the agent to adhere to the requirements of the GDPR when processing the personal data.

The lack of specific steps means businesses need to consider the personal data they hold, how they process it and ensure they have policies in place to comply with the principles. The authorities will want to see businesses are aware of and seeking to comply with their responsibilities. This could be done by having written policies and giving staff training on how to comply with the policies.

Lawful Processing

The processing has to be lawful. The GDPR allows personal data to be processed with consent. There must be some form of clear affirmative action to denote consent – a positive opt-in. Consent cannot be inferred from silence, pre-ticked boxes or inactivity. The consent must be kept separate from other terms and conditions and there must be a simple procedure to allow that consent to be withdrawn if the data subject wishes to do so. This would be important for example where collecting personal data for marketing reasons.

Where electronic mailing lists are used, consent through an active form of communication, such as an opt-in tick box, should be provided at the time the consent is collected. With each communication the person receiving the communication should then be given the opportunity to opt-out.

However, consent is just one basis for the lawful processing. Processing is also lawful if it is, for example:

- necessary for entering into or performing a contract;
- necessary to comply with a legal obligation; or
- necessary to protect vital interests of a data subject.

If you hold personal data for managing tenancies you could rely on the fact the data is necessary for entering into or performing the contracts or complying with your legal obligations. If a contractor gives you personal data so you can contact them for future work it may be that the justification for processing is that it is necessary for entering into a contract.

Privacy Notices

The GDPR introduces requirements as to the information which needs to be supplied when obtaining personal data. Normally this information is included in a privacy notice.

The information which needs to be supplied depends on whether the personal data was obtained directly or from a third party. Where it is obtained directly then the information must be given at that time – where it is obtained indirectly then it must generally be supplied within one month.

For example if people provide personal data via your website, then you can provide the privacy notice on your website. If tenants provide personal data when applying for a tenancy, you can provide a privacy notice when you collect that information.

Rights of Data Subjects

The "Data Subject" is the person whose information you hold. Data subjects have various rights which include

- rights of access to personal data;
- the right to have personal data rectified if it is inaccurate or incomplete;
- a right to require personal data to be deleted;
- a right to block processing; and
- a right to object to processing.

If a data subject requests access to personal data this will usually have to be supplied free of charge and within one month of receipt of the request.

There is a right to erasure ('right to be forgotten') but this will only apply if one of a number of grounds apply.

When a data subject challenges the accuracy of the personal data held about him/her, a data subject will be able to exercise his/her right under the GDPR to restrict the processing. A restriction of processing will mean that processing can only take place in very limited circumstances, otherwise the personal data must be stored until the restriction is lifted.

The GDPR introduces a new right to data portability. In certain circumstances data subjects will have the right to obtain and reuse their personal data for their own purposes. In these cases you will be required to provide the personal data in a structured, commonly used and machine readable form. This must be supplied free of charge within one month.

If your business has personal databases for marketing or to manage significant tenancy portfolios then you should have a policy for how you deal with the exercise of the rights of data subjects.

Breach Notification

The GDPR will introduce a duty to report certain types of personal data breach to the relevant authority (in the case of the UK, this is the Information Commissioner's Office) and in some cases to the data subjects who are affected by the breach.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

This type of breach will only have to be notified to the Information Commissioner's Office where it is likely to result in a significant detrimental effect on the data subject, such as discrimination, damage to reputation, financial loss or loss of confidentiality. You must notify any such breach without undue delay and in any event within 72 hours after becoming aware of it (unless there are very good reasons for any delay).

You will only need to report the breach to the data subjects themselves if there is a high risk to their rights and freedoms. This threshold is higher than that for reporting to the supervisory authority. The GDPR specifies the details that must be included in any notification and your procedures for dealing with a personal data breach must be updated to take account of these.

Recommended Actions

The ICO recommend that data controllers take action now to prepare themselves for the GDPR. The ICO's advice includes:

- making sure that the relevant people are aware of the GDPR and its implications;
- be clear about the personal data you hold, where it came from and who you share it with;
- review any privacy notices;

- checking your procedures in dealing with data subject access requests;
- identifying the lawful basis upon which you currently process personal data and;
- if you are relying on consent whether new consents are required;
- checking your procedures for dealing with data breaches;
- designating somebody in your organisation to take responsibility for data protection compliance; and
- ensuring that compliance with the GDPR, for example implementing necessary security measures, is taken into account by your organisation from the design stage of any new service or technology (where the processing of personal data is to be carried out) through to when delivering that technology or service.

Application of the GDPR to other organisations

Even small organisations such as churches and small charities will need to consider and adhere to the GDPR.

Where these organisations seek donations from the wider public they will need to, amongst other things:

- have a justification for obtaining and holding the personal data of donees or potential donees. Practically, this means that organisations will need to have thought about these considerations and have an 'audit trail' of their reasoning which can be provided to the ICO, if required. Where that justification is the consent of the data subject to be contacted, the consent must be obtained through an active communication, for example an opt-in tick box on an electronic form;
- provide privacy notices to data subjects containing all the required 'fair processing information';
- consider how they hold recorded personal data and have appropriate technical and organisational measures to ensure that the personal data is secure. Those measures must be appropriate, taking into account the form of the processing (practically, what is appropriate will take into account the nature and context of the processing; and presumably the ICO will not expect a church to have the same resources as a social media giant); measures need not be expensive if it can be justified to the ICO that the measures were appropriate;
- manage the records to be processed, including deleting personal data when it is no longer necessary for the reason it was collected and responding to the rights of data subjects; and
- consider appointing or allocating responsibility to a representative to manage the personal data and the responsibilities of the organisation under the GDPR, for example responding to requests from data subjects.

Administrative Fines

Failure to comply with the GDPR may result in fines being imposed by the ICO, although the ICO has indicated that any fines would be proportionate to the nature and extent of the non-compliance. The maximum fines that can be imposed will be up to 2 % of worldwide annual turnover (or €10 million) for certain breaches of the GDPR and up to 4 % of worldwide annual turnover (or €20 million) for other, some may say, more serious breaches.

Individual data subjects will have a right to claim compensation from you if your breach of the GDPR has caused them to suffer any damage, and they may complain to the ICO. There is also likely to be unwelcome publicity and potential damage to reputation in these circumstances.

Andrew Priest

Partner
Cambridge
01223 532746
andrewpriest@hewitsons.com

We pride ourselves on delivering an outstanding service to a wide range of individuals, businesses and institutions including charities, educational and sports bodies. The firm's size and breadth of specialisms means each client receives the focus it requires. We operate UK wide and have worldwide reach via our network of independent law firms, LawExchange International.