General Data Protection Regulation (GDPR) Fact Sheet

The General Data Protection Regulations (GDPR) came into force in 25 May 2018. It will replace the existing Data Protection Acts and creates a new regime for handling individual's personal data. This will be supplemented in the UK by a new Data Protection Act which is currently passing through Parliament which should be in force before May.

WHO DOES THIS APPLY TO?

The GDPR applies to any organisation in the European Union that handles personal data. It will also apply to any organisation outside the EU which handles data from EU citizens. Even though the UK will be leaving the EU we are obliged to comply with EU regulations during the time until we leave and UK nationals would be able to rely on the GDPR even if the UK government was to ignore it.

Even when we leave the EU we will likely continue to operate a virtually identical regime as the UK was a big supporter of the GDPR regime and will need to have a similar level of protection of personal data if it wants to trade with the EU.

WHY IS THIS HAPPENING?

At the moment the data protection rights of individuals are fragmented as each EU country has slightly different laws, albeit following an overarching directive. In addition, the data protection regime is outdated and does not deal with modern data usage. Individual data now commonly crosses borders being collected in one country, stored in another, and processed in a third. A lot of data is now processed automatically with decisions being made entirely by computer algorithms without substantial human intervention. In addition, a lot of data is now collected autonomously by observing behaviour, such as where we go with our mobile phones and what services we use in different locations. None of these issues are dealt with effectively under current legislation and GDPR aims to assist with these.

DATA SUBJECTS AND DATA RIGHTS

The GDPR gives data subjects, the people whose personal data is being used, rights to control the use of their data and rights to know what is being done with it. These rights are not dissimilar to the existing ones under the current Data Protection Acts but they are more detailed and require greater levels of transparency.

WHAT IS ALL THIS ABOUT CONSENT?

For many data controllers the biggest issue will be changes to consent. It is necessary to have consent for the use of any data. In some cases this consent can be implied where it is necessary to complete the terms of a contract with the person whose data is involved or where it is necessary to protect the vital interests of the person holding the data. These will cover a lot of the work being carried out by property agents. However, such implied consent will not allow for the collection of data for marketing purposes and consent for this will need to be given by the individual data subject. In addition, consent must be specific and granular. This means that consent must be for a clear and specified purpose and where consent is given for one thing you cannot then add a lot of additional items to that consent. So, for example, where I instruct an agent to let or sell my house I will give consent to the use of data for that purpose on an implied basis. However, I cannot be required to give my consent to being contacted for marketing purposes; this must be given separately and explicitly.

All requests for consent must also be specific. This means that consent which is being asked for must be given explicitly and cannot be collected by a clause in an agreement which says that I consent or by a pre-ticked box on a form. I must actively give my agreement. In addition, I am entitled to withdraw my consent at any time and this must be respected and all data for which my consent can be legitimately withdrawn must be deleted. I cannot withdraw consent for areas in which consent is implied unless I am also removing your obligations. So if the lettings terms of business have a termination clause within them I can terminate the contract and ask you to delete the data you were retaining in reliance on the implied consent for performance of a contract. However, I cannot make you delete data you are holding to protect your vital interests.

WHAT IS PERSONAL DATA?

The definition of personal data is not changed. So, data that can identify me as an individual is personal. This is the case even if the data does not identify me by name. So if the data identifies me specifically, then that will be personal data as it can be tied to a clearly identifiable individual. Some data, relating to nationality, health, sexual preferences and the like is especially sensitive. This is called special category data and the consent to process this is much harder to obtain. Property agents should not find themselves dealing with special category data and the government is taking steps to exempt data collected for Right to Rent purposes from this category.

Business data is not normally seen as personal data. So, if you hold my work email address and are using it for the purposes of dealing with me in a business context for my job role then that will not be personal data. However, if you are using my work email address to sell me personal services then it will be personal data and covered by the GDPR.

WHAT ABOUT DATA WE ALREADY HOLD?

If you already hold data subject to existing data protection regimes then it will fall under the GDPR. This means that consent to a GDPR standard will need to exist for that data to continue to be held. This may already exist as an implied consent but for data that is being held for marketing purposes implied consent cannot be given and so explicit consent will have to be held.

Where explicit consent is needed then this will have to exist to the standard required by GDPR and so it will need to be opt-in consent and clearly specify the use to which the data is being put (as opposed to a more blanket consent). It is very unlikely that existing marketing data will have consent to a GDPR standard. Therefore, it will need to be deleted on 25 May unless it has had consent to GDPR standards in the meantime.

DATA TRANSPARENCY

A key element of the GDPR is being very clear with people where their data is going and what is being done with it. This includes specifying precisely what third party organisations and countries the data is being sent to and what they will do with it. For letting agents & landlords this will mean a much tighter relationship with referencing agents for example who processes personal data at the direction of the agent or landlord to make decisions about tenancies.

The GDPR envisages every data subject receiving a privacy notice specifying what is being done with their data and who is doing it. This is a key part of the consent regime. A starting point in creating such a notice is to conduct a Privacy Impact Assessment (also known as a Data Protection Impact Assessment) to set out what is done with data and the risks to individual data subjects of their rights being violated.

DOCUMENTS AND POLICIES

GDPR requires data protection to be embedded in the design of policies and processes. It is important therefore to have policies as to how data is to be used and protected. These policies are required to be written down. For smaller organisations of less than 250 employees it is only necessary to document regular data processing activity. At a minimum you should be documenting:

• The name and contact details of your organisation, your data protection officer, and third parties who process data for you (e.g tenant referencing agencies);

- The purposes of your data processing;

• A description of the type of individuals you process data about and the categories of personal data you are processing for them;

• Who receives personal data processed by you;

• Any transfer of data to another country including how this is done and what security is in place to protect that data and ensure it is not misused;

• How long data is kept for;

• The security you have in place to protect data, both physical and IT security.

It would also be sensible to have documentation for the following areas:

- records of consent;
- contracts with organisations processing data at your direction;
- the location of personal data;
- Privacy Impact Assessments;
- records of personal data breaches;

DATA PROTECTION OFFICERS

The GDPR requires larger organisations or those who are routinely processing a lot of data to have a Data Protection Officer (DPO) who is responsible for ensuring compliance with the GDPR. At the current time the government Data Protection Bill goes further and requires every organisation to have a DPO. A DPO must be appropriately trained to conduct their role and so will need to be very familiar with the requirements of the GDPR.

DATA PROTECTION OFFICERS Contd.

While they do not need to be on the main board or management team of an organisation they should be clearly consulted whenever a decision is being made that may involve data protection issues and written evidence of that should be kept. A DPO cannot lose their job for carrying out any aspect of their function, including making reports to the appropriate data protection authorities and so they will need appropriate clauses in their employment contract to protect them. Organisations do not need to have their own DPO in house and they are allowed to share them. So several small businesses could club together to share a DPO between them.

REPORTING AND ENFORCEMENT

Where a data breach occurs such that personal data is lost, destroyed, or disclosed inappropriately then it must be reported to the appropriate data protection authority if it is serious. A serious breach is one that will impact on one or more individuals in terms of their privacy, reputation or financial status. Minor matters do not need to be notified. So the loss of an internal staff telephone list is unlikely to require notification while the loss of a person's bank details is. Notifications to the authorities must occur within 72 hours of the discovery of the breach and in the UK the appropriate authority is the Information Commissioner. If the breach creates a high risk to individuals then they must be personally notified as well but this threshold is higher than the obligation to notify the authorities. There is no set time limit on notifications to individuals but this must happen without undue delay.

If there is a data breach or there is any failure to comply with a part of the GDPR then the authorities can levy fines and individuals can take their own legal proceedings to seek damages. The levels of fine are much increased under GDPR and can go up to 10 million euros or 2% of annual worldwide turnover, whichever is the greater for lesser offences or 20 million euros or 4% of annual worldwide turnover, whichever is the greater for more serious matters.