FAQ: An introduction to GDPR

What is GDPR?

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations across the region approach data privacy.

Like its predecessor, the GDPR is designed to protect personally identifiable information (personal data).

What is its purpose?

Protecting citizens personal data. Technology has continued to grow since the EU Data Protection Directive of 1995, giving companies new ways of using and sharing the personal data that they collect. The need to protect individuals whilst making the legislation more widely standardised across the EU was deemed to be so important that this new regulation was developed.

Establishing a single European law for data protection will remove barriers to cross-border trade, enabling businesses to expand more easily across Europe. Currently, businesses in the EU have to deal with 28 different data protection laws, making it harder for small companies in particular to access new markets. The new rules will remove the current obligation for businesses to notify other national data protection authorities about the data they are processing, which currently costs them about €130 million per year. The overall cost savings as a result of reducing this red tape are estimated at some €2.3 bn per year.

At the same time, organizations can use the GDPR as a way to separate themselves from competitors by placing an emphasis on transparency in order to build trust with customers and potential clients.

What constitutes personal data?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. The legislation applies not only to electronic data but any records that are stored in a form that is easily searchable.

For property companies, this could, for example, include data relating to investors, fund managers, valuations, compliance, bookkeeping, payroll, background checks and human resources.

Who does it affect and when does it apply?

Although the regulation was published in May 2016 the law will not apply to organisations until 25 May 2018 in the European Union.

One of the biggest changes compared with the previous legislation is the new law's broader remit.

For those in the UK, regardless of Brexit, the adoption of GDPR will go ahead and although each jurisdiction does have the ability to make minor local adjustments it's not anticipated that these will change the impact of GDPR for all EU members.

If your organisation is based outside the EU, the legislation still applies to you if you offer goods, provide services or even just process the data of an EU citizen - whether they are residing in the EU at the time or not. This is one of the bigger changes to the previous legislation and means that essentially most organisations must prepare to adhere to the new rules.

What about small companies?

The GDPR expects all small and medium-sized enterprises (SMEs) to comply in full with the Regulation, but it does make exceptions for organisations that have fewer than 250 employees.

The Regulation acknowledges that SMEs generate a lower risk to the privacy of data subjects than larger organisations. For example, Article 30 of the Regulation states that organisations with fewer than 250 employees are not required to maintain a record of processing activities under its responsibility, unless “the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data […] or personal data relating to criminal convictions and offences”.

It should be noted that private individuals not engaged in business activities are exempt. You’re free, at home, to store personal contact details without the overheads that the GDPR enforce - providing, of course, this is for personal use only.

However, even with these concessions, it is important that each organisation, whatever its size, takes its responsibilities seriously.

GDPR key changes

Among the main changes under GDPR, compared to previous directive:

Increased Territorial Scope (extra-territorial applicability)

The biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company’s location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to “result in a risk for the rights and freedoms of individuals”. This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.

Right to Access

Under the GDPR, individuals will have the right to obtain confirmation that their data is being processed; access to their personal data; and other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Right to be Forgotten

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At it Is core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall implement appropriate technical and organisational measures in an effective way, in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local Data Protection Authorities, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements.) Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

How will GDPR affect surveying practices?

For a chartered surveying firm, here are just a few of the types of data that will be covered by GPDR:

- Data you hold to service your clients, for example:
    - Data in your valuation systems
    - Data in your compliance systems, including accounts, bookkeeping, payroll and HR data
- Any working papers that support your compliance work which contain personal data
- Any customer data you hold for marketing purposes
- Emails and correspondence, both internal and external, since many of these will relate to clients and to their employees and will therefore contain personal data
- It's not just electronic data. Any records that are stored in a form that is easily searchable can fall under the remit of regulation.

GDPR imposes obligations on you in relation to this data. In summary:

- You must have knowledge of the data you store and process, its geography (where it resides), security usage and composition:
    - Is it personal, prohibited, client-related or employee-related?
    - How is it captured - is it permitted by law and by the client?
- You must be able to provide information on how the data is used and on the rights of individuals regarding their data
- You must demonstrate that you are managing personal data in a manner compliant with the regulations and be able to supply, on request, the details of the data you hold and how it has been used
- You have to be able to delete every instance of an individual's data in compliance with the right to be forgotten (including data held in backups)
- You must offer this data in a format that allows portability to other data processors should the need arise.

Who regulates the GDPR?

It's important to note that the RICS does not regulate the provision of GDPR or the existing act and that each jurisdiction has its own Data Protection Authorities (DPA). Below is a table of the major European points of contact:

Find your National Data Protection Authority online

Breaches

A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Under the new regulations data breaches must be reported to the national regulator but only where it is likely to result in a risk to the rights and freedoms of individuals. The test to consider is if unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Breaches are typically discovered through access logs, reported thefts, lost equipment or a data security incident that involves personal data.

This initial report must be made within 72 hours of having become aware of it. And to clarify - these hours don't stop for weekends and evenings. You'll have longer to compile a full report if required but you must make the ICO aware within those first 3 days.

What are the maximum penalties?

If your organisation is found to be non-compliant there are fines of up to 4% of its annual worldwide turnover or €20 million, whichever is greater. This is the maximum fine that can be imposed for the most serious infringements (e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts). There is a tiered approach to fines (e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Best Practice to be compliant with the new GDPR:

1. **First of all – don't panic!** The foundation of data protection rules is still the same as before.
2. **Conduct a data review:** A data audit to understand risks, access rights, purpose for storing the data, clarifying your rights to ensure you have consent to store the data (more importantly, the right to store the data for the purpose in which you are using it).
3. **Anonymise data wherever possible**: Every instance of real personal data is a potential breach risk. Test systems should not contain actual customer data and be very aware of data analytics which contain references to identifiable people.
4. **Encrypt everything (wherever possible):** Laptops and memory sticks are the easiest way for data to leave the organisation. PCs are stolen, left on trains and in taxis and memory sticks are often mislaid – it is easy for the hard-drives of stolen equipment to be mined for personal data if they are not encrypted. Obtain the correct documentation when disposing of assets (a simple format of a hard drive may not be enough to remove data) and remember that the security of personal data is your organisation's responsibility throughout.
5. **Create a Breach Response Policy:** Knowing the team that will respond, the lines of communications, the recovery procedures and the documentation required is essential to getting the organisation on-track in the event of a breach or data-disaster.
6. **Understand the Data Subject Request process**: A plan should be in place to handle client's requests for data or changes to this data. This procedure is run when a person asks for the information that your organisation holds about them in relation to a specific topic, invokes the right to be forgotten or simply requests you update the data you hold on them. The regulation provides an organisation just one month from receipt of the request to provide a response to the requester and this response must be robust and complete. Don't forget your obligations to verify the requester is who they claim to be and that in disclosing any information you are not infringing the rights of other data subjects.
7. **It's more than just personal data**: The GDPR is primarily responsible for personal data. This means that corporate data does not fall under its remit. RICS firmly believes that the surveying profession must treat sensitive commercial data in largely the same way as personal data. A robust data handling policy will encompass all aspects of your organisation's data and in return your client data will be more secure.
8. **Consider the data landscape:** Employee's personal devices, if they are using them for business purposes, fall within the scope of the GDPR so it is important that your organisation policies include provisions for personal devices to ensure that all employees are compliant.

   The GDPR, and any related regulation (e.g. the EU ePrivacy Regulation) are designed to make the data environment a safe place for personal data but it will not eradicate breaches or data-disasters. Knowing your processes, your people's responsibilities and the organisation's remit is the best way to keep the regulators, and more importantly, your clients on your side.
9. **Data storage**: If you store data, remember that GDPR does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

> *"Data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');"*

This is deliberately vague as there is a huge array of data, covered by the regulations, which is processed for different purposes. The question an individual / firm needs to consider is why they believe necessary to continue to hold personal information). In practice, it means that firms need to:

- review the length of time personal data is kept;
- consider the purpose or purposes the information is held when deciding whether (and for how long) to retain it. For instance; Is there an insurance requirement, industry requirement, or sources that stipulate minimum retention periods, such as local laws etc.
- securely destroy information that is no longer needed for this purpose, or these purposes;

Remember that retained data should only be used for the purpose it was originally collected for. If it is to be used for another purpose make sure there is a legal basis to do so

Does my business need to appoint a Data Protection Officer (DPO)?

DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

What is the difference between a data processor and a data controller?

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

What about Data Subjects under the age of 16?

Parental consent will be required to process the personal data of children under the age of 16 for online services; member states may legislate for a lower age of consent but this will not be below the age of 13.

What is the difference between a regulation and a directive?

A regulation is a binding legislative act. It must be applied in its entirety across the EU, while a directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast the the previous legislation, which is a directive.