General Data Protection Regulation (GDPR)

What you need to know
Complying with data protection regulation is an essential part of running any successful business. With the General Data Protection Regulation (GDPR) effective from 25 May 2018, replacing the Data Protection Act (DPA) 1998, you need to understand the implications for your business and take measures to be compliant to avoid potential fines which can be crippling under the new regime.

It is important to remember that the GDPR's main principals are very similar to those under the DPA, and if you are following best practice guidance already, then updating and documenting internal data processes will be relatively straightforward.

For more detailed information see the links below:
- The Information Commissioner's Office (ICO) which proposes '12 Steps to Take Now' and includes an 'Implementation Checklists' for each key issue. https://ico.org.uk/media/2014146/gdpr-12-steps-infographic-201705.pdf https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- ACAS: acas.org.uk/
- The Data Protection Network: https://dpnetwork.org.uk/

Data Protection Principles
Article 5 of the GDPR requires that personal data (defined as data from which a living individual can be identified, including email address) shall be:
- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedom of individuals;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The ICO has produced a Guide to Data Protection (https://ico.org.uk/for-organisations/guide-to-data-protection/) that explains these principles in more detail.

Project data
As a practitioner it is likely that you will be processing personal data as part of your project work. Examples of such personal data may include:
- Names
- Addresses
- Email addresses
- Geolocation data
- Data that relates to an individual person (separate from others in their group) is likely to be personal data

Examples of ways in which you might process data when working on a project:
- In emails and letters
- In the project brief
- On drawings (physical and PDF/other digital media)
- In models on common data environments/clouds
- In visualisations
- In strategy documents

The GDPR requires you to have a lawful ground to process personal data. For project purposes this will generally fall under the lawful ground known as 'legitimate interest', because the individual(s) commissioning the project would naturally expect you to process their data in order to deliver the project. Using that same data for an unrelated purpose, such as sharing it with a marketing agency, would not be 'legitimate interest'.

Personal data processed pursuant to a contract (appointment) is also likely to be lawful processing. Where there has been a contractual relationship between the parties, it is permissible to make further contact with the individual for new leads, provided an opportunity to be removed from any marketing list is offered at the same time. Under any other circumstance, your practice should seek consent from individuals whose

personal data they collect and administer in any way. Consent must be 'informed', so it is important to explain exactly what it will be processed for at the outset. Consent can be revoked at any time (for instance using an 'unsubscribe' function) so it is important to refresh the consent for processing an individual's personal data, on a regular basis.

It is also recommended that all drawings, models, information, data and correspondence should be retained from initial contact with your client through to the end of the limitation period (6 or 12 years post contract/practical completion) and any limitation extension. The purpose of this is to be able to respond to any legal claim or similar. However, under the GDPR, personal data may need to be erased earlier than this, if there ceases to be any 'legitimate interest' to process the data. This is the principle of 'data minimisation' under the GDPR. The GDPR requires data processors to ensure they implement secure systems to protect personal data, and requires that any external parties which process personal data for your practice also take reasonable precautions to safeguard personal data.

The GDPR includes a requirement for organisations to begin new projects or offer new services with data protection built in at the outset rather than bolted on as an afterthought; this requirement is also known as Data Privacy by Design. To ensure you can demonstrate that your practice meets this requirement, prior to starting work, you may wish to undertake a data protection impact assessment to determine what data you need to process throughout the project, why it needs to be processed and how you will be processing it. This will help identify all the individuals you may need consent from if they do not fall under 'legitimate interest'.

Marketing
The most important data your practice will need to process outside of a project will be for marketing and human resources purposes.

You and your practice should have a privacy policy on your website, as a form of 'Privacy Notice', that includes a section on data retention for marketing purposes.

The ICO has guidance and examples of Privacy Notices in Practice.

When engaging in direct marketing, consent must be 'freely given, specific, informed and unambiguous' i.e. a positive opt-in, and consent cannot be inferred from inactivity. You must also enable an unsubscribe option from future marketing.

The ICO has also published guidance on Preventing direct marketing.

Human resources/recruitment
There is a considerable amount of guidance available online for employers to consider regarding securing the personal data of employees. Again, the ICO has detailed guidance on employment.

END

This copy revised and updated September 2020. It supersedes all previous versions of this document.

Chartered Institute of Architectural Technologists
397 City Road, London EC1V 1NH
T: +44 (0)20 7278 2206
practice@ciat.global
architecturaltechnology.com
Twitter: @ciatechnologist
Instagram: @ciatechnologist
Facebook: ciatechnologist