

GDPR POLICY

Introduction:

The EU General Data Protection Regulation (GDPR) was approved in 2016 and will become directly applicable as law in the UK as from 25th May 2018. The current Data Protection Bill, which will become the Data Protection Act 2018 (DPA 18), fills in the gaps in the GDPR, addressing areas in which flexibility and derogations are permitted.

The GDPR will not be directly applicable in the UK post Brexit but the DPA18 will ensure continuity by putting in place the same data protection regime in UK law pre-and post-Brexit, equivalent to that introduced by the GDPR which will continue to be applicable throughout the EU member states.

The Bill does not replicate all of the provisions of the GDPR but cross-refers to the relevant provisions as appropriate. When the GDPR and DPA18 come into force, it will therefore be necessary to view the DPA18 and the GDPR side by side in order to see the complete picture of all the data protection legislation. The guidance note only refers to the relevant provisions of all the data protection legislation, once the DPA18 comes into force. The guidance will also be kept up to date in light of any relevant guidance issued from Government and the Information Commissioner's Office (ICO)

The GDPR requires we, as a Company, nominate Controllers that process personal data demonstrate compliance with its provisions. Part of this involves establishing and publishing a basis for lawful processing and where relevant, a condition for processing special categories of data.

Consent is one of a number of options to meet each of these requirements under GDPR

Establishing a lawful basis under the GDPR:

As controllers under the GDPR, organisations that process personal data must establish and publish the lawful basis that they are relying on for processing that data.

The GDPR sets out conditions for lawful processing of personal data (Article 6) and further conditions for processing special categories of personal data (Article 9). These are similar to the conditions in schedules 2&3 of the Data Protection Act 1998 (DPA98) with sensitive personal data now called *special categories* of personal data.

Confidentiality requirements are unaffected:

The fact consent may be obtained for confidentiality purposes does not mean that consent must also be the lawful basis applied for the purposes of data processing in compliance with the GDPR. Well established national guidance on confidentiality remains applicable.

Consent under GDPR:

In the limited circumstances that consent is the only or most appropriate condition to use as the lawful basis for processing, organisations must periodically consider the practical implications such as ensuring the consent is valid for GDPR purposes.

Consent must be given freely, specific, informed and unambiguous

The client can withdraw their consent at any given time however they must be aware of the implications in doing so.

The ICO suggests explicit consent must be expressly confirmed and recorded in writing, in a very clear and specific statement.