The New General Data Protection Regulation (GDPR) and Contracts

What's new?

The GDPR builds on existing data protection laws. It provides enhanced protection for personal data and imposes stricter obligations on those who process personal data. The new obligations include:

- When an individual's personal data is collected, they must be given more information about how it will be used through enhanced privacy notices.
- Individuals will have much stronger rights to have their personal data corrected, erased and/or provided to them.

What is personal data?

Personal data is any information that relates to an identified or identifiable living person (e.g. staff member, member of the public, or Service user). It generally includes their name, address, phone number, date of birth, place of birth, place of work, opinions, opinions about them, whether they are members of a trade union, their political beliefs, ethnicity, religion or sexuality (as well as other information about them). Information which indirectly identifies a person will also be personal data. This would be the case where a single piece of information could not be used to identify a person but could do so in combination with other data or identifiers.

Who needs to comply with the new requirements?

The GDPR applies to both 'Data Controllers' and 'Data Processors'. A Data Controller is the person/ organisation which, solely or with others, determine the purposes and means of processing personal data. A Data Processor is the person/organisation which processes the personal data on behalf of the Data Controller. In most of the Authority's contracts, the Authority is the Data Controller and the Contractor (supplier) is the Data Processor.

Processing to meet the requirements of the regulation

Data Controllers may only appoint Data Processors who provide sufficient guarantees over appropriate technical and organisational measures to ensure processing meets the requirements of GDPR. Data Processors are required to process personal data in accordance with the Data Controller's instructions (to include a Schedule of Processing). It is in the interest of both Data Controller and Data Processor to make sure obligations are set out as clearly as possible.

Restrictions on Sub-Contracting

GDPR gives Data Controllers a wide degree of control in terms of the ability of the Data Processor to sub-contract. Data Processors require prior written consent from the Data Controller. The Data Processor is required to inform the Data Controller of any new sub-processors, giving the Data Controller time to object. If there is an objection, the sub-processing may not continue.

The lead Data Processor in a sub-contracting arrangement is required to reflect the same contractual obligations it has with the Data Controller in a contract with any sub-processors, and remains liable to the Data Controller for the actions or inactions of any sub-processor.

Data Controller / Data Processor contract

Data Processor activities must be governed by a binding contract. The binding obligations on the Data Processor must cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the Data Controller (as also set out within a Schedule of Processing). There are a number of specific requirements including that the personal data is processed only on documented instructions from the Data Controller, and requirements to assist the Data Controller in complying with many of its obligations. The Data Processor has an obligation to tell the Data Controller if it believes that the Data Controller's instructions infringe the GDPR, or any other law.

Demonstrating compliance

GDPR requires organisations to demonstrate compliance. Data Processors are under an obligation to maintain a record of all categories of processing activities. These records must be provided to the Information Commissioner's Office on request, and must include details of:

- the Data Controllers they act for
- any other processors
- a Data Protection Officer (DPO)
- the categories of processing carried out
- details of any transfers to third countries
- a general description of technical and organisational security measures.

Data Processors must assess their need to comply by understanding whether they have fewer than 250 employees. If so, and unless the processing does not pose a risk to the rights and freedoms of individuals, is not more than occasional, and does not include special categories of data (sensitive personal data), then the requirements are reduced.

Security

Data Processors, like Data Controllers, are required to implement 'appropriate' security measures. What is 'appropriate' is assessed in terms of a variety of factors including the sensitivity of the data, the risks to individuals associated with any processing or breaches of security, the state of the current available technologies, the costs of implementation and the nature of the processing. These measures might include pseudonymisation and encryption. Regular testing of the effectiveness of any security measures is also required where appropriate.

Breach notification

Data Processors are required to notify their relevant Data Controller of any breach without undue delay after becoming aware of it. Data Controllers have 72 hours to notify the Information Commissioner's Office from the point the breach is detected, therefore, reporting from the Data Processor to the Data Controller is required well within this time period. **Avon Fire Authority expects that a breach is notified to us within 24 hours of it being detected. Contractors can do this by contacting the AF&RS Service Control on 0117 926 2061 Extension: 311/312.**

Data Protection Officers

Both Data Controllers and Data Processors are required to appoint DPOs in certain situations, including where they are a public authority or body, where the data processing activities require regular monitoring of data subjects on a large scale, or where the core activities of the processing involve large amounts of special (sensitive) data or data relating to criminal convictions and offences. The primary role of the DPO is to ensure compliance with the GDPR. Data Processors may also choose to appoint a DPO even if they do not fall into one of the specified categories.

Rights to information

Data subjects have an increased right to the information held about them under GDPR, including the right to copies of their personal data without charge (Subject Access Request), greater transparency about the processing carried out with their data (for example the legal basis for processing, retention periods, data sharing arrangements), and a reduced timeframe for a response to a Subject Access Request (now 30 calendar days).

If your organisation receives a Subject Access Request for data processed on behalf of Avon Fire Authority/ Avon Fire & Rescue Service, we expect the request to be passed to us within no more than 3 working days from receipt. You are expected to assist with any requests from Avon Fire Authority/ Avon Fire & Rescue Service for any personal data processed on our behalf, in response to a Subject Access Request, within no more than 5 working days. The data should be passed to us in its complete and unredacted form.

Transfers to third countries

The Data Processor has to exercise a degree of independence from the Data Controller when deciding whether or not it can transfer personal data to a third country. While Data Processors are required to follow the relevant Data Controller's instructions with regard to the data processing, no matter what those instructions are, they may only transfer personal data to a third country (in the absence of an adequacy decision) if the Data Controller or Data Processor has provided appropriate safeguards, and on condition that data subjects have enforceable rights in that country with respect to the data.