0800 243 919 secretary@chsa.co.uk www.chsa.co.uk

chsa
cleaning & hygiene suppliers association
www.chsa.co.uk

The GDPR: a quick overview

What is the GDPR?

The GDPR is the General Data Protection Regulation which comes into force across the EU on 25 May 2018. Organisations must be GDPR compliant from this date.

The Information Commissioner's Office (ICO) which regulates these matters has pointed out that two years' notice has been given of the change and lack of time to implement change is unlikely to be accepted as an excuse. In practice many businesses will not be fully compliant by 25 May but it will be essential to show full engagement with the process and a realistic action plan to become compliant.

Compliance will be an ongoing process. New technologies will emerge and working practices will change. Businesses must constantly review their data protection strategy to ensure that they remain compliant. 25 May is an important date in the process but it must not be seen as the endpoint.

The GDPR covers the processing of 'personal data' that relates to 'data subjects' by or on behalf of a 'data controller'. For members, this means it affects how you hold, use and access data. HR, business development and marketing are likely to be affected in your business.

Key definitions

Personal Data	**any information relating to an identified or identifiable individual (the Data Subject).**
Data Subject	**the person who can be identified, directly or indirectly, by the data held.**
Data Processing	**almost any operation performed on Personal Data, including deleting it or simply putting it in a spreadsheet.**
Data Controller	**the entity who determines the purposes and means of processing the data.**
Data Processor	**the processor of the data on behalf of the Data Controller. This can be a sub-contractor, for example a marketing company targeting an email campaign at prospects.**
Supervisory Authority	**the UK supervisory authority is the Information Commissioner's Office ("ICO").**

What are the responsibilities of the Data Controller?

The Data Controller must be able to prove to the ICO that it is adhering to the data acquisition and management guidelines and regulations. Data Controllers must ensure that they have adopted policies, procedures and technical measures to keep Personal Data secure.

The regulations include the following six principles regarding the processing of Personal Data.

Personal Data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is required for the purposes for which they are processed;
- accurate and kept up to date;
- not kept for longer than is necessary; and
- processed in an appropriately secure manner including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

The right to be forgotten is important to note. This means that organisations are responsible for deleting or removing outdated or inaccurate Personal Data. You should, therefore, ensure that you are not holding any Personal Data which you no longer require or which contains incorrect information. It is best practice to ensure that you have a written data retention policy in place to deal with the length of time Personal Data will be held for and its deletion.

There are further responsibilities for organisations with more than 250 employees, including the maintenance of relevant records and documentation.

Particular care should be taken if any Personal Data is sent outside of the European Economic Area as more stringent rules must be adhered to.

There are also special rules which govern "Sensitive Data". Sensitive Data includes, amongst other things, a persons' religious, cultural and/or political beliefs and details about their health, sexual orientation and/or sex life.

What are the duties of a Data Processor?

Any suppliers or sub-contractors processing data on your behalf must provide guarantees to implement measures that meet your obligations as Data Controller. This means that you must ensure that written contracts are in place setting out the necessary obligations and requirements. Any existing contracts in place between you and Data Processors will need to be updated so that they are GDPR compliant on its implementation.

Data Processing is generally unlawful unless it falls within one of the six legitimising conditions. The conditions most likely to be relevant to members of the CHSA are:

Consent
The Data Subject has given clear consent to the processing of his or her Personal Data for one or more specific purposes. The consent must be freely given, informed and unambiguous and must be capable of being withdrawn.

Performance of a contract
The data Processing is necessary for the performance of a contract with or on behalf of the Data Subject.

Legitimate interests
The processing is necessary for the purposes of a legitimate interest of the Data Controller or a third party EXCEPT where such interest is overridden by the fundamental rights and freedoms of the Data Subject which require the protection of Personal Data.

Subject access requests

Under current law, Data Subjects have the right to request that you provide them with details of all information you hold about them. At present you have 40 calendar days to respond to such a request. You may also charge the Data Subject for your compliance (up to a maximum capped fee).

Under the GDPR, the time you have to comply with a request will be reduced to 30 days. You are also not able to charge for complying with a request, unless the request is manifestly unfounded or excessive. You are also able to refuse to comply with a request in certain, limited, circumstances.

Mailing lists

Generally, an active opt-in is required for marketing as you must ensure that you have express consent reinforced by a 'clear, affirmative action'. This means that you are unable to rely on implied permission and, therefore, pre-ticked boxes that automatically opt customers in unless they uncheck them will no longer be sufficient. It may be good practice to rely on a double opt-in for new subscribers. This means that new subscribers who sign up to a mailing list via a contact form automatically receive a verification email with an activation link to the address provided by the new subscriber. The email address is added to the mailing list only when the link is clicked.

Consent via an active opt-in is not required if you are emailing marketing information about similar products or services to existing customers or clients as long as you give them an ongoing opportunity to opt-out. This only applies if the customer or client has previously opted-in to receive such marketing emails.

Inactive or silent members on the mailing list are not giving consent to be on the list. It is good practice to confirm membership of your marketing lists annually, although you should not contact any person that has previously opted-out (or, alternatively, not opted-in) to receiving such correspondence. This is considered spam mail and could lead to you being fined by the ICO.

Data Subjects must understand what they are giving consent to by signing up to a mailing list, so make the language clear and simple.

Data breaches

It is important that Data Controllers notify the ICO of any data breaches within 72 hours of awareness if such breach is likely to result in a risk to the rights or freedoms of Data Subjects. If there is a high risk to such rights and freedoms, the Data Controller must also notify any affected Data Subjects without delay. Examples of breaches that would require notification are breaches which may cause Data Subjects financial loss, affect their confidentiality or lead to identity theft.
A failure to notify the ICO of a relevant data breach may incur a fine in addition to any fine imposed for the data breach itself.

What are the penalties?

The ICO has a range of powers to ensure compliance. These include issuing warnings and ordering the notification of a Personal Data breach to the Data Subject(s).

Fines can be also be imposed. The current maximum of £500,000 is increased to

- up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher
- a fine of up to €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year for the most severe forms of a breach
- The level of the fine will depend on the nature, gravity and duration of the infringement and clearly the highest level of fines will only be levied for the most serious and egregious breaches. Fines under the existing legislation have however been very significant and the risk of a fine must not be disregarded.

It is important to note that the burden of proof will shift on the implementation of the GDPR. Whilst currently a Data Subject will need to demonstrate that their Personal Data has been mishandled, the GDPR requires that Data Controllers be able to prove that they are compliant with the legislation.

This document provides a basic overview of the GDPR. More information is available on the ICO website (ico.org.uk) including the 'Getting ready for the GDPR checklist' and '12 steps to take now'.

Data protection is a complex area with its application often fact dependant. This note is not intended to be relied on as comprehensive legal advice. If you have any queries or issues relating to data protection, or about getting ready for the GDPR, you should seek legal advice.

You may wish to contact Lester Aldridge LLP who assisted in the preparation of this note by contacting Geoff Trobridge on 01202 786138 or at Geoff.trobridge@la-law.com or Edward Adamson on 01202 786115 or at edward.adamson@la-law.com.