ARE YOU GDPR READY

Overview

The **General Data Protection Regulation** is an important piece of legislation adopted by the European Parliament and the European Council. It will be brought in on the 25th May 2018, and it will give greater strength and consistency to the Data Protection given to individuals.
It will enable EU Citizens greater control over the personal information that companies hold about them. It will also give companies a more concise and uncomplicated set of rules to follow when handling personal data.

As the UK will still be part of the EU when this legislation comes into force, companies will need to comply. Prior to this date it is essential that businesses are prepared. By taking action now it will ensure that you are fully compliant and can ensure against potential data breaches and will also assure your employees and customers that you take their data protection seriously.

12 Steps to take now.

1. **AWARENESS.** Make sure that decision makers and key people in your organization are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. **INFORMATION YOU HOLD.** You should document what personal data you hold, where it came from and who you share it with. You may need to organize an information audit.

3. **COMMUNICATING PRIVACY INFORMATION**. You should review your current privacy notices and put a plan in place for making any necessary changes in time for the GDPR implementation.

4. **INDIVIDUALS RIGHTS**. You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. **SUBJECT ACCESS REQUESTS**. You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information

6. **LAWFUL BASIS FOR PROCESSING PERSONAL DATA.** You should identify the lawful basis for processing activity in the GDPR, document it and update your privacy notice to explain it.

7. **CONSENT**. You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR Standard

8. **CHILDREN**. You should start thinking now about whether you need to put systems in place to verify individual's ages and to obtain parental or guardian consent for any data processing activity.

9. **DATA BREACHES**. You should make sure that you have the correct procedures in place to detect, report and investigate a personal data breach.

10. **DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS**. You should familiarize yourself now with ICO's Code of Practice on Privacy Impact Assessments as well as the latest Guidance on Article 29 Working Party, and work out how and when to implement them into your organization

11. **DATA PROTECTION OFFICERS.** You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organizations structure and governance arrangements You should consider whether you are required to formally designate a Data Protection Officer.

12. **INTERNATIONAL.** If your organization operates in more than one EU member state (i.e. if you carry out cross-border processing) you should determine your lead data protection supervisory authority. Article 29 – Working Part Guidelines will help you do this.

More detailed information can be found at
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Breach of GDPR Regulations would be costly!

Depending on the precise nature of the breach, the ICO will have the authority to fine companies up to 20 Million Euros, or 4% of their global turnover. But aside from this financial cost implication, a breach in the GDPR Regulations would have an significant impact on your company's reputation and loss of customer confidence.

Examples of Personal Data

Recorded information about an identifiable individual that may include his or her: -

(1) name, address, email address, phone number,
(2) race, nationality, ethnicity, origin, color, religious or political beliefs or associations,
(3) age, sex, sexual orientation, marital status, family status,
(4) identifying number, code, symbol,
(5) finger prints, blood type, inherited characteristics,
(6) health care history including information on physical/mental disability,
(7) educational, financial, criminal, employment history,
(8) others' opinion about the individual, and
(9) personal views except those about other individuals

How Secure destruction of personal data help organizations to comply with the regulation.

Organizations must have a data retention policy, as its one of the requirements of the GDPR that details of this policy are notified to data subjects. In accordance with the accountability principle referred to above, organizations must be able to demonstrate compliance with their own data retention polices. Secure destruction protocols must be part of your internal processing procedures to ensure compliance to the GDPR.

The importance of using a reputable Data Destruction Company.

The section highlights the importance of information destruction for businesses and the benefits of using a quality supplier. With identity fraud rising, sensitive information and data needs to be destroyed properly otherwise confidential details can be put at risk.
The ID section's work is particularly relevant to the Data Protection Act. Every Data Controller using an information destruction company is required to choose a supplier which provides sufficient guarantees of security measures, including destruction being carried out under contract and evidenced in writing.
Evergreen Secure Shredding work to a European Standard for the secure destruction of confidential material (EN 15713) as part of their ISO 9001:2008 inspection.

OUR COMMITMENT AND SERVICE TO YOU

We service a number of high-profile Customers.

We are passionate about the level of service we provide and the range of services we can offer. We are able to shred a wide range of materials and products i.e. paper, cardboard, branded merchandise, I.T Equipment, CD's Data Tapes, X-Rays< Microfiche, redundant stock etc….. Giving our customers total peace of mind that they are disposing of items in a safe, secure and legal manner.

Evergreen Secure Shredding are members of SAFEContractor and have attained ISO9001 & 14001 accreditation.

We provide both On-site (mobile) and off-site secure shredding and recycling services to many customers and pride ourselves in our proactive approach to offering a first-class service. We are, and have always been, an ethical, reliable and sustainable service provider to a wide range of business and strive to offer a proactive approach to individual's needs.

The new regulations focus on internal processes and risks and how these contributing factors are documented and assessed. Making sure you have a compliant asset disposal company acting as your data processor is crucial to avoiding risks with your data. GDPR requires that data processors must:

- Have a detailed service agreement with the data controller.
- Provide sufficient guarantees, in terms of expert knowledge and ability to deliver the service; including appropriate technical and organisational measures. (e.g. site audit annual compliance documentation etc)
- Adhere to an approved code of conduct (e.g. BSEN15713 destruction standards incorporated within an QMS such as 9001).
- Adhere to an approved certification mechanism. (e.g. BSIA ID approved member)
- Regularly test, assess and evaluate the effectiveness of their measures to ensure the security of processing. (e.g. regular testing incorporated within the UKAS auditing of the ISO QMS certification)
- Be dedicated to notifying the controller without undue delay after becoming aware of a personal data breach.

Customer compliance assured with a COD (Certificate of Destruction) issued, following the secure destruction of your confidential material, (sample statement of compliance below).

CERTIFICATE OF DESTRUCTION

GDPR Ready

Evergreen Secure Shredding have shredded and recycled this consignment in accordance with the Information Destruction Standards BS EN15713 which is vetted within our ISO9001 & 14001 quality management systems. Providing the customer legal compliance, and best practice in accordance to the Data Protection Act, (Physical security with approved technical security measures to handle waste paper and computerised records). GDPR (General Data Protection Regulations) which supersedes the DPA on the 25th May 2018. GDPR requires that organisations carry out Privacy Impact Assessments (PIAs), to access areas of risk. This Certificate of Destruction is an important control document the Data Protection Officer can use to demonstrate compliance, in conjunction with a service agreement.

Helpful guidance available at - www. ico.org.uk/for-organisations/data-protection-reform.

More detailed information can be found at: -

- Information Commissioners Office (ICO) www.ico.org.uk
- British Security Industry Association www.bsia.co.uk/sections/information-destruction.aspx
- CPNI www.cpni.gov.uk
- Evergreen Secure Shredding www.evergreenshredding.co.uk

Please contact us for helpful advice on our Security Shredding Services;

Shaun Vowles (Manager)
Tel. 0117 9828090
Email – shaun@evergreenshredding.co.uk