GDPR

GDPR & Retail

sfb CONSULTING GROUP

GDPR

The General Data Protection Regulation ('GDPR') comes into effect on 25 May 2018

It will affect all organisations which hold personal data about EU citizens.

The majority of organisations will beaffected by the legislative changes.

Membership Organisations generally hold a significant amount of personal data regarding their members, employees and other persons.

Under GDPR, organisations face large fines for any improper use of personal data or a breach of data protection legislation, which is primarily enforced in the UK by the Information Commissioner's Office.

"Don't be frightened by GDPR - it is an excellent opportunity for you to review and renew one of your organisation's most valuable assets, namely your personal databases."

sfb CONSULTING GROUP

GDPR

It is important that you ensure that your databases which include personal data, are reviewed prior to 25.5.18, in order to ensure that your organisation can continue to use them, once GDPR comes into effect.

You should be thinking about the following issues regarding areas of data holdings:

- Employment records
- Client/Customer databases
- Third party suppliers

You must also ensure that the terms and conditions with people and organisations, with whom you share personal data, are GDPR compliant.

SFB CONSULTING GROUP

Summary of the GDPR General Principles Relating to the Processing of Personal Data (Article 5)

1. It must be processed lawfully, fairly and in a transparent manner, in relation to the individual.
2. It must be collected for specified, explicit and legitimate purposes.
3. It must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.
4. It must be accurate.
5. It must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes.
6. It must be processed in a manner that ensures appropriate security of the personal data.

Also note that data controllers are obliged to implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for a specific purpose of the processing are processed (Art 25).

Both data controllers and data processors are responsible for ensuring that personal data is processed in accordance with GDPR.

GDPR

Generally, there are six grounds for lawful processing of personal data:

1. Consent (Art 6(1)(a) - Rec 32, 42 & 43))
2. Contractual necessity (Art 6(1)(b) - Rec 44)
3. Compliance with legal obligation (Art 6(1)(c) - Rec 45)
4. Vital interests (Art 6(1)(d) - Rec 46)
5. Public interest (Art 6(1)(e) - Rec 45)
6. Legitimate interest (Art 6(1)(f) - Rec 47 & 48)

You need to record the lawful basis for processing personal data, for example in appropriate policies and procedures.

GDPR

So what now?

Here are some proposed first steps towards compliance:

- Ensure that all third party suppliers (such as accountants and publishers) are GDPR compliant before you transfer personal data to them, and that your terms and conditions reflect this
- Define, in your data protection policy, the legal basis for processing personal data
- Obtain GDPR compliant consent, if you are relying upon this legal basis for processing personal data
- Revise your Privacy Notice, so that it is GDPR compliant, and ensure that this is communicated

- Consider whether your organisation needs a Data Protection Officer;
- Review your IT and office security
- Ensure that both management and staff are aware of the changes to the law
- Ensure that your organisation has the appropriate systems in place in order to cover the individual's rights under GDPR (such as Subject Access Requests and the right to be forgotten)
- Consider whether any personal data which you hold is transferred internationally, and, if so, ensure that appropriate controls are in place

sfb CONSULTING GROUP

Marketing

Many Retailer will be able to rely upon contractual necessity for processing personal data, but this would not necessarily cover general direct marketing materials.

If you are sending direct marketing materials to your clients and customers or others, you will probably need GDPR compliant consent for such marketing.

In order to obtain GDPR valid consent, your organisation will need to inform the person from whom you are receiving consent, that they have the right to withdraw their consent at any time.

You will need to obtain specific consent as to the means by which you wish to communicate with them (e.g. by mail, post, telephone etc).

You also need to advise them on each occasion when you contact them, after you have received consent, of their right to withdraw their consent, so as not to invalidate the consent.

Don't forget to record how and when you obtained consent.

Phone : 0800 699 0533
Email : letstalk@sfbconsulting.co.uk
Web : www.sfbconsulting.co.uk

SFB CONSULTING GROUP