GDPR ADVICE
FOR EMPLOYEES OF
SMALL AND MEDIUM
SIZED BUSINESSES

stonehewermoss

SOLICITORS

GDPR ADVICE FOR EMPLOYEES OF SMALL AND MEDIUM SIZED BUSINESSES

Purpose

The purpose of this leaflet is to provide advice to employees of smaller businesses who are in need of training in respect of how the GDPR will apply to them and the organisation they work for.

What Is Changing ?

The Current law protecting information that organisations hold about individuals (or Data Subjects) is contained in the Data Protection Act 1998. This will be placed by the General Data Protection Regulations or GDPR on 25th May 2018. These regulations are due to be brought into force in the UK by the Data Protection Act 2018 and accordingly they will not be substantially affected by Brexit.

Supervision of the regulations and enforcement of GDPR is the responsibility of the Information Commission or ICO. The law places responsibilities on the organisation you work for as the user of Personal Data. As such your organisation will be a Data Controller. However the regulations also apply to you as an employee. Failing to process data legally can be a criminal offence. The consequence for the organisation you work for of a breach of data can be very serious and it can be ordered to pay large fines (up to 4% of the turnover if the previous year or 20 Million Euros, whichever is the larger) and for this reason employees who cause a breach may be subject to disciplinary proceedings.

What is Processing Personal Data ?

Personal Data is any information that can be linked to a living individual anywhere in the world. This might be a name, images recorded on CCTV, an ID number, personal email or even an IP address. Processing Personal Data includes just having it in your possession, so an unused PC in a store cupboard still counts so long as there is Personal Data on it even if that is just one name. No organisation can process Personal Data without a reason, such as consent of the Data Subject, legal obligation of the Data Controller, or with a view to entering into a contract with the Data Subject. A full list of the six reasons can be found under Article 6 of the GDPR.

For the sake of completeness it should be mentioned that the GDPR applies to individuals not just companies unless the data is for ‘purely personal’ reasons. This includes pictures and information posted on social media so if you post a photograph of your friend on Facebook you are processing Personal Data.

The Principles of the GDPR

Having defined Personal Data and what is meant by processing the GDPR sets out the Principles of data processing which must be complied with. The Personal Data must be processed bearing in mind the following principles of Article 5 of the GDPR:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

- Accountability

However for most purposes you only need to ask:

1. Is the information needed? (lawful, fair, purpose)

When collecting data the organisation you work for should only ask for and process data that is relevant for its purpose. For example you would not ask for someone's shoe size if they were booking a hotel room. The data collected should be the minimum needed and not obtained for the sake of it.

2. Is it accurate?

The data held should be correct. Incorrect data can lead to loss to the Data Subject. For example if you record a person as bankrupt but then fail to update your organisations records when the bankruptcy is lifted you would not be processing accurate data and this might to lead to loss if the Data Subject applied for a mortgage and was turned down. This could then be the fault of your organisation.

3. Is it secure? (integrity and confidentiality)

Your organisation is responsible for preventing the loss of Personal Data by unauthorised access to it through, security measure and corporate procedures. Be careful who you pass data on to, check first if they are within the EU and if you have a legitimate reason to share the data you hold with that organisation. For example, if you work in accounts and you need to pass your colleague's details to an external payroll organisation, this would probably be lawful. Passing the same details to marketing organisation in the USA without reason would probably not be. Be careful with emails. It is very easy to send large amounts of Personal Data by email to other organisations without first thinking about whether or not it was lawful.

4. Would you mind the person seeing it (transparency, fairness, accurate, purpose)

The Data Subject is entitled to ask for all the Personal Data that your organisation holds in relation to him or her. This is so they can check what is held is accurate and is being processed lawfully. The Data Subject can object under the GDPR if the Personal Data is inaccurate, being processed without need or unfairly. If you need to make critical records about a Data Subject you should choose your language carefully as they have a right to see everything. It is an offence to change, amend or update data after you have received a subject access request. If, in a file, you record phrases like 'this customer is a nightmare' you might be in the embarrassing situation of having to hand the note over to them after Data Subject Access Request.

What is Special Data ?

If your organisation processes what used to be called sensitive personal information then you have enhanced responsibilities to the Data Subjects.

Special data is listed as being any data relating to:

- racial or ethnic origin
- political opinions

- religious or philosophical beliefs
- trade union membership
- data concerning health or sex life and sexual orientation;
- genetic data
- biometric data where processed to uniquely identify a person (not photographs generally)

Special Personal Data does not does not include criminal records although for many practical purposes it should be treated as the same.

Your organisation must have lawful reasons for recording and processing special Personal Data, such as for the purpose of legal proceedings, with explicit consent of the Data Subject or for employment law obligations. Your organisation will also have one of the reasons under Article 6. The full list of the reasons which allow your organisation to process special Personal Data can be found in Article 9 of the GDPR.

Data Protection and Freedom of Information

These two areas are very different but are often considered together as they are both supervised by the Information Commissioners Office. The two can be summarised as follows. The GDPR gives members of the public the right to see Personal Data about themselves, held by an organisation but not right to see data about another person. For example you could ask the Licencing Authority for details they hold about your television licence but you could not ask to see your neighbour's information.

The Freedom of Information Act gives individuals the right to see information held by public bodies but not the right to see any Personal Data. For example you can ask the licencing authority about how many television licences they issued but you could not ask who paid for them. Freedom of information does not extend to private companies, so, you could not require a large burger chain to provide you with statistics about how many burgers they sell a year.

What do we mean by data Privacy ?

The terms 'data privacy' and 'privacy policy' can sometimes be confusing. The right to privacy has many limitations and privacy policies state how your data will be used as well as how it will be kept secure. For example when you purchase a policy of car insurance the insurance organisation are under a legal obligation to inform Driver and Vehicle Licence Agency you have done so. Under the GDPR you cannot object to this. Other instances where a Data Subject may no longer have the right to object to their Data being processed are civil and criminal legal cases, matters of national security and processing involving journalism or freedom of expression.

Following implementation of the GDPR most organisations should have a written Fair Data Use Policy (or privacy policy) to provide transparency to the Data Subjects.

Privacy & Electronic Communications Regulations (PECR)

Sending of marketing, emails, faxes, texts and even cookies, is strictly regulated within the EU under this regulation, which is why most spam is sent from outside the EU. Anyone who uses electronic means to market must comply with the rule. They must also comply with the obligations of the

GDPR. These obligations apply to companies operating outside the EU if they are marketing to people within the EU although enforcement may be an issue. PECR is due to be replaced by new eprivacy regulations.

General Duty of Confidentiality

Long before the GDPR there is a tradition of confidentiality between certain professions and Data Subjects such as doctor and patient or solicitor and client. If your organisation owes a duty of confidentiality to people to whom it provides services then this will work hand in hand with the GDPR and will not conflict with it.

Legal Disclosure

There are circumstances when it is allowed or even a legal requirement to disclose Personal Data. For example the Criminal Records Bureau disclose information about convicted offenders to certain authorised employers especially where employment brings the person into contact with children. Such disclosures are specified exemptions under the GDPR and the regulations state that these powers are controlled and subject to specific provisions as to the manner of the processing.

Brexit

Further Reading

If you want to find out more about how the GDPR and The Data Protection Act 20018 might affect you as an employee of a smaller business a good place to start would be the website for the Information commissioner which can be found at ico.org.uk

DISCLAIMER:

The content of this note is provided for general information only. It is not intended to amount to advice on which you should or can rely. You must obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of this note.