PROFILING AND MARKETING

The GDPR introduces the concept of 'profiling'. This is related to automated decision making (which appears in both the Data Protection Act 1998 and the GDPR). Profiling involves processing which:

- occurs automatically
- evaluates personal aspects of a natural person
- is used to analyse /predict behaviour or characteristics

Where profiling occurs, data subjects should be informed how and why it occurs. Extra conditions (such as a need for explicit consent or for the processing to relate to the entering into of a contract) apply if the profiling results in a legal effect on or adverse consequence for the data subject.

This new requirement is likely to impact marketing, where profiling plays and an important role. Note also that electronic marketing (e.g. by email) will be affected by proposed reforms to the EU's electronic privacy regime which are expected to be finalised in 2017 and enter into force in 2018.

DATA PROTECTION OFFICERS

Data protection officers ("DPO") have to be appointed by:

- local authorities
- organisations monitoring individual's behavior
- organisations processing sensitive data on a large scale
- In other cases a DPO is not required, but is still good practice.

The DPO must be an expert in data protection law and have a degree of independence (i.e. it shouldn't be anyone heavily involved in managing an organisation's data processes such as an IT manager).

PRIVACY IMPACT ASSESSMENTS

Privacy impact assessments, which were already good practice under the Data Protection Act 1998, are now a legal requirement where processing (particularly processing involving new technologies) is likely to result in a high risk to individuals' rights in relation to their personal data.

RECORD KEEPING

The GDPR requires controllers (and processors) keep detailed records about their processing activities.

Amongst other things, these must contain the categories of personal data processed, security measures, recipients of personal data transfers. Record keeping obligations are in addition to need to demonstrate compliance elsewhere (e.g. the accountability principle).

INTERNATIONAL DATA TRANSFERS

Both the DPA 1998 and the GDPR generally prohibit the transfer of personal data outside the EEA, subject to a few exceptions.

The rules under GDPR are broadly the same, though it will also be possible to transfer personal data under accredited certification schemes or approved codes of conduct to. Keep in mind that measures to comply with under the DPA 1998's transfer restrictions (e.g. EU model contracts) may need to be revised and updated when the GDPR comes into force.

SECURITY

What security the GDPR requires depends on the risks in question and what is proportionate. Security remain based around appropriate technical and organisational measures must be implemented to protect personal data, against theft, unauthorised access, loss, damage and destruction.

What is "appropriate" depends on the nature of the personal data (and the harm that would result from a data breach), but it may include encryption and pseudonymisation.

BREACH REPORTING

The DPA does not legally require data controllers or processors to notify the ICO (or affected data subjects) of a personal data breach, though the ICO expects serious breaches to be notified to it.

The GDPR will require:

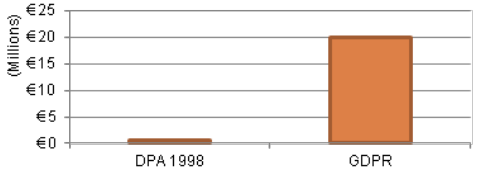
- controllers notify all breaches to the ICO within 72 hours unless the breach is unlikely to endanger the rights and freedoms of data subjects
- controllers notify severe breaches to affected data subjects
- processors notify breaches to controllers

All organisations will need personal data breach and notification policies in place in order to be able to react quickly.

FINES

In the UK fines for breaching the Data Protection Act 1998 can be up to £500,000. The GDPR will introduce fines of up to €20m or 4% of group worldwide turnover

These fines are in addition to the threat of civil claims from data subjects and/or from representative bodies (such as consumer organisations).



QUESTIONS?

Oliver Neil

Solicitor , Data Protection and Privacy
Tel: 01865 781 219
E: oliver.neil@freeths.co.uk

Oliver Neil is a solicitor with particular expertise in commercial data protection law. He works with clients across a range of industries, including financial services providers, supermarkets, building materials producers, global non-profit organisations, logistics companies, hotel chains and email service providers.

Some examples of how Oliver has recently used his data protection expertise to help clients are:

- a secondment to one of the UK's largest charities, to manage the legal aspects of their GDPR compliance programme;
- advising on subject access request responses and disclosure obligations;
- helping clients implement standard contracts to legally transfer personal data outside the EEA;
- advising on remedial action and notification obligations following a data breach;
- negotiating data protection warranties and indemnities;
- advising clients on data processing and data sub-processing outside the EEA;
- preparing data sharing agreements between controllers;
- drafting privacy policies, privacy notices and opt-in statements; and
- advising on direct marketing under the DPA 1998, PECR and GDPR.

01865 781000 www.freethsoxford.co.uk

FREETHS
SOLICITORS

General Data Protection Regulation Card

5000 Oxford Business Park South
Oxford OX4 2BH

01865 781000

www.freethsoxford.co.uk

INTRODUCTION

This data card is intended to highlight some of the key parts of the General Data Protection Regulation ("GDPR").

The GDPR will result in better protection for individuals, but will increase the compliance obligations on organisations. The potential fines for breaching the law will also increase significantly.

What is the GDPR?	The General Data Protection Regulation (Regulation (EU) 2016/679) is an EU law which is a directly applicable to the whole of the UK
When is in force?	25 May 2018
Who will it apply to?	All persons and organisations which control or process personal data
Where will it apply?	The GDPR will be implemented in all European Economic Area (EEA) states, but it will apply persons and organisations outside the EEA which control or process the personal data of European nationals
What are the maximum fines?	€20m or 4% of worldwide group turnover (whichever is higher)
Is there a transition period?	Yes, a two year transition period started in 2016 and will end on 24 May 2018. Organisations will be expected to be fully compliant with the GDPR when it comes into force
Where can I find further information?	The Information Commissioners Office (ICO) publishes information and guidance on its website (www.ico.org.uk). You can also contact Freeths' data protection solicitors who are experts in this area

EVOLUTION NOT REVOLUTION

The GDPR will completely overhaul the UK's data protection regime and introduce much better protection for individuals (and stricter obligations for controllers and processors).

Although the GDPR brings in a number of major changes, much of it is not completely new. Instead, it adds to, reinforces and clarifies obligations that already exist under the Data Protection Act 1998. In that way it is very much an evolution of data protection law rather than a revolution.

What used to be best practice will become a legal requirement and, in order to succeed, controllers and processors need to embrace the GDPR and ensure respect for personal data. Those who only do the minimum necessary and try to cut corners will find compliance a constant battle and are more likely to fail.

BREXIT

Brexit will not prevent the GDPR from coming into force. The UK will still be a member of European Union when the GDPR becomes effective on 25 May 2018. The UK Government and ICO have made clear their intention that the GDPR (or an equivalent regime) will continue to apply if the UK leaves the EU.

At the moment it is not clear if and how European Union court judgments relating to data protection will be implemented in the UK. Other cross border issues (such as cooperation between data protection authorities, the UK's role in the EU data protection board) also remain uncertain.

WHAT IS PERSONAL DATA?

The GPDR applies to processing (a broad term which includes any use, storage, transfer and deletion) of personal data.

Personal data (typically) includes any information relating to a living individual who can be identified. The term is broadly defined and can cover anything from basic personal information (e.g. name, address, NI number, telephone, email) to complex data such as IP addresses, biometric information and geo-location data. It is not limited to confidential or sensitive data.

SPECIAL CATEGORIES OF DATA

Additional obligations and conditions apply to the following categories of personal data (previously known as sensitive data):

- racial/ethnic origin
- religious/philosophical beliefs
- trade union membership
- genetic/biometric data (processed for identification purposes)
- health
- information relating to an individual's sex life or sexual orientation.

Some personal data (such as financial information) may not fall within a special category but will still require additional security due to its nature and the harm that would result from a personal data breach.

CONTROLLER / PROCESSOR

The GDPR divides persons (including organisations) which handle personal data into two categories:

- Controllers – who determine the "means and purposes" of processing (i.e. control of how and why personal data is used)
- Processors – who process data on behalf of (and under the instructions of) a controller

The majority of responsibility (and liability) rests with the controller. However, under the GDPR, processors can also be liable.

DATA PROTECTION PRINCIPLES

The Data Protection Act ("DPA") 1998 requires organisations to comply with eight principles (and certain specific obligations, such as responding to subject access requests). The GPDR retains this approach, but consolidates the existing principles. In summary, the GDPR requires personal data are:

- processed lawfully, fairly and transparently
- only collected and used for particular lawful purposes
- adequate, relevant and not excessive for that purpose
- accurate and up to date
- stored no longer than necessary
- kept secure, and its integrity and confidentiality are protected

There is also a new accountability principle, which means you need to be able demonstrate compliance with these principles.

CONTRACTING

An important change under GDPR is that any processing of personal data (e.g. by suppliers, contractors, service providers) has to be carried out under a written contract which meets the criteria set out in Article 28 of the GDPR.

Amongst other things, the contract must address:

- international transfers
- only acting on the controller's instructions
- confidentiality
- sub-processing restrictions
- security obligations
- deletion of data
- provision of information
- audits and inspections
- responding to requests by data subjects

Any processing must be carried out pursuant to a contract which meets the requirements of Article 28 or it will be unlawful. Standard contracts and processor policies will need to be revised well in advance of the GDPR to ensure contracts are valid when the new law comes into force.

01865 781000 www.freethsoxford.co.uk

CONSENT

The threshold for consent is much higher under the GDPR than the DPA 1998. Under the GDPR, for processing to be based on the data subject's consent, the controller must be able to demonstrate that consent. Any requests for consent must be clearly distinguishable from other matters, intelligible and easily accessible and clear and plain language.

Consent requires a freely given, specific, informed, unambiguous indication of wishes by statement or clear affirmative action. In practice, if consent is needed, anything less than an express opt-in is unlikely to be sufficient.

Keep in mind that consent:

- can be withdrawn (and you must make it easy to do so)
- is not always appropriate (e.g. if you would process the data anyway)
- won't be valid if there is too much of an imbalance of power (e.g. if an employer asks an employee for consent)
- needs to remain valid (meaning it may need to be refreshed)

Consents which don't meet the requirements of the GDPR cannot be relied on from 25 May 2018 meaning that, unless other grounds for processing exist, fresh (valid) consent needs to be obtained by that date or else you must cease processing.

LAWFUL PROCESSING

Personal data can only be processed where there are lawful grounds for doing so. This includes that processing is carried out with the data subject's consent or is necessary in order to:

- to perform or enter into a contract with the data subject
- for the controller to comply with a legal obligation
- to protect the vital interests of the data subject
- for the controller's legitimate interests, provided these are not overridden by the interests or rights of the data subject

Public bodies cannot rely on the legitimate interests ground, but can process personal data where it is necessary for the public interest or in the exercise of their official authority.

DATA SUBJECT

Under both the Data Protection Act 1998 and the GDPR data subjects have a right to access their personal data. However, the GDPR will alter the subject access request (SAR) process. The changes include the following:

- the SAR response deadline is reduced from 40 days to 30 days
- no fee can be charged (except for excessive, repetitive requests etc.)
- additional information on data subject rights must be provided

To comply with these changes, data controllers should ensure their SAR procedures and template responses are updated.

The GDPR also retains a data subject's right to object (including to his or personal data being used for direct marketing or automated decision making) and have inaccurate personal data rectified.
The GDPR introduces the following rights:

- the right to erasure (also known as the right to be forgotten) which allows a data subject to require his or her personal data be deleted (subject to some exceptions)
- the right to data portability entitling data subjects to a copy of any personal data he or she has provided and which is processed automatically on the basis of consent or performance of a contract. This data should be provided in a structured common electronic format where it is feasible to do so
- a right to restrict processing in certain situations

01865 781000 www.freethsoxford.co.uk