MACFARLANES

EU DATA PROTECTION REFORMS

A REVIEW OF THE KEY IMPACTS AND HOW TO PREPARE FOR THEM

OVERVIEW

Facebook builds up valuable data based on its users' clicks, likes and comments; brands then pay Facebook to target users based on their age, location and interests. Just one example of the possession, use and sharing of personal data becoming the common currency of modern commerce. However, sophisticated cyber attacks and instances of large scale data loss have increasingly made headlines and badly damaged reputations (e.g. Sony Playstation, Talk Talk and Ashley Madison).

It is therefore essential that businesses understand and engage with the stricter new data protection regime they are going to be subject to, so as to avoid the potentially severe financial and reputational damage which can result from getting it wrong.

In 1995, the EU introduced the Data Protection Directive (the Directive) to regulate how EU residents' "personal data" could be collected, used and moved within the EU[1]. The Directive was not directly effective in each member state but instead allowed differing interpretations and levels of protection between the member states.

The Directive will shortly be replaced by the new General Data Protection Regulation (the GDPR) which will: (i) reflect developments in technology; (ii) lead to consistency of data protection regimes across Europe; (iii) apply to more businesses than the previous Directive; (iv) place more complicated and onerous obligations on each of these businesses; and (v) increase the fines for non-compliance to up to four per cent of an organisation's global turnover.

The new GDPR is likely to make data protection a key governance issue alongside the likes of bribery, health and safety and FCA regulation/compliance. It will nominally "come into force" on 24 May 2016 and businesses are required to be compliant by 25 May 2018 (i.e. there is a grace period for businesses to make the necessary changes to their organisations). In order to ensure compliance with the GDPR, businesses should conduct a detailed audit to determine what type of personal data they hold, where this data is held and what they use it for.

To prepare for the GDPR, businesses must act now to: (i) familiarise themselves with the new regime; (ii) raise awareness within their organisation; (iii) allocate adequate budgets and staff; (iv) begin documenting the types of personal data their organisation holds; and (v) put in place the requisite procedures and safeguards.

This booklet summarises:

- the core framework of the current Directive;
- the key changes to be implemented by the GDPR;
- the implications for businesses of those changes; and
- the action businesses should now be taking to prepare for the GDPR's introduction.

[1] The Directive also applies to the European Economic Area countries - Iceland, Liechtenstein and Norway

THE FRAMEWORK OF THE EXISTING DIRECTIVE

The Directive regulates the manner in which people and entities (data controllers) can collect "personal data" relating to individuals (data subjects) and how they may use and distribute such information whilst it is under their control (known as processing). The Directive applies to data controllers who are established within the EU (including branch offices) or who process personal data within the EU (e.g. via computer servers located within the EU). It therefore captures almost every business operating in the EU in one way or another. Common examples of potential data subjects include a business' existing or potential clients and its employees, contractors and suppliers.

DEFINITIONS

- **Data controller** – "*a natural or legal person, public authority, agency or any other body which […] determines the purposes and means of the processing of personal data*" i.e. the entity which controls the data and decides what data is collected, how it is stored and how it is used. This is in contrast to a third party (such as an IT service provider) which processes personal data on the instructions of another (known as a "**data processor**").
- **Personal data** – "*any information relating to an identified or identifiable natural person*" e.g. a person's name, contact details, education history, medical records, employment details, financial details and purchasing history. Personal data can be in either electronic or manual/paper format and need not be information which is confidential to the individual. Data relating to companies or legal entities is not caught by this definition.
- **Processing** – "*any operation or set of operations which is performed upon personal data*" i.e. includes collection, storage, alteration, use, disclosure or destruction of personal data (almost any action will be treated as processing).

DATA CONTROLLERS' OBLIGATIONS

- To inform national authorities (before processing) what information the controller intends to collect, about whom and why, how this will be kept secure and where (or to whom) this information might be transferred/disclosed.
- To comply with certain principles such as: only processing personal data fairly and lawfully; collecting and using data only for specified and legitimate purposes; ensuring that all data held is accurate and up to date; and keeping data in a form which doesn't allow identification of data subjects for longer than is necessary.
- To only process personal data if, for example: the data subject has consented; it is necessary for compliance with a legal obligation (e.g. a court order); or it is necessary for the data controller's legitimate interests.
- To implement technical and organisational measures to prevent: accidental loss, disclosure or destruction of personal data; unlawful processing; and unauthorised access to personal data.
- To ensure that their data processors (e.g. website hosts) also implement appropriate security measures and that the contracts in place between the data controller and data processor provide for this.
- Not to transfer personal data outside the EU unless the recipient country ensures an "adequate level of protection" for the data.

RIGHTS OF DATA SUBJECTS

- To be provided on request with a copy of any personal data that a data controller holds about them.
- To object to processing of their personal data in certain circumstances (e.g. for direct marketing).
- Not to have decisions made about them based solely on the automated processing of personal data (e.g. decisions about creditworthiness, work performance etc.).
- To obtain compensation from data controllers for losses suffered as a result of unlawful processing of personal data.
- To have enhanced security/protection for their "sensitive personal data" which includes, for example, information regarding racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, health or sex life.
- To object to processing of their personal data which is inaccurate or incomplete (and to request erasure or rectification of this data).

THE GDPR:
THE KEY CHANGES

Application

The GDPR will be directly applicable and enforceable in the EU and EEA countries (whereas the Directive was not directly enforceable, leading to differences in implementation and interpretation). This will standardise data protection law across Europe and may make it easier for multinational companies to manage the personal data they hold. Data controllers will be regulated by a lead enforcement authority in the member state where they are most established.

Action *– Although businesses do not need to be compliant with the GDPR until May 2018, the steps necessary to ensure compliance could take years to implement and the costs of compliance could be significant. Businesses should now: (i) appoint someone to supervise compliance and oversee the transition; (ii) identify their lead data protection authority (this normally being the authority in the country in which the controller or processor has its main establishment) and, if appropriate, open a dialogue with that authority; and (iii) ensure sufficient budget and other resources are allocated to introduce the new systems and processes.*

Enhanced collection requirements

Data controllers will need to provide additional information to data subjects at the point of collection in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language*", for example information regarding:

- how long personal data will be retained;
- the data subjects' rights to withdraw consent to processing and/or lodge a complaint with the data protection authority;
- whether the data controller processes personal data for profiling purposes and, if so, the "*significance and the envisaged consequences of such processing*"; and
- the safeguards which the data controller has in place for any envisaged international transfers of personal data.

Action *– Businesses should review/update their privacy policies to ensure that the information provided to customers/data subjects is clearly presented and not written in impenetrable or overly legalistic language. Lengthy, small and dense text contained in an attachment to an email, for instance, is unlikely to be considered "concise, transparent, intelligible and easily accessible".*

"Consent" to processing

Under the GDPR:

- a data subject's consent to processing must be "*freely given, specific, informed and unambiguous*" and shown "*either by a statement or by a clear affirmative action*". It is unlikely that consent will be freely given if it is a condition of the contract (i.e. take it or leave it);

- consent to the processing of sensitive personal data (e.g. information revealing racial origin, political or religious opinions or concerning the individual's health or sex life) must be explicit (i.e. it cannot be implied);
- the data controller will have the burden of proving that the data subject consented to any processing and that this consent was properly obtained;
- a data subject may withdraw their consent to processing at any time (e.g. to stop direct marketing); and
- businesses will need to demonstrate that parental/guardian consent has been obtained to process data of children under the age of 16. Member states have discretion to lower this age to 13.

***Action** – Businesses should evaluate how they seek, obtain and record data subjects' consent to processing. In particular, "opt-out" boxes on websites may not always suffice. Any consent given as a precondition to entry into a contract is also unlikely to be "freely given" (and should not be relied upon).*

Data subjects' consent must now be given "either by a statement or by a clear affirmative action" so implied consent becomes harder to demonstrate. Data controllers must retain evidence that data subjects have positively consented to the purposes for which their data is being used and put procedures in place to delete data when consent is withdrawn.

Given that consent can be withdrawn, data controllers may find it preferable to use other grounds to justify processing, for example, if they can demonstrate that the processing is necessary for the legitimate interests of the data controller (e.g. where a customer has stopped making payments under a loan agreement, the finance company might disclose their personal data to a debt collection agency).

It could be argued that an employee cannot ever "freely give" their consent to an employer's processing of their personal data since such consent is likely to be a pre-condition of employment, e.g. all employees must agree to the company data security policy which allows the company to monitor their work emails to detect data breaches. Businesses should therefore consider justifying processing in an employment context using one of the other exemptions (e.g. the processing is necessary for the data controller's legitimate interests).

Businesses which are targeted at children (e.g. social networking) should implement procedures to verify the data subject's age and obtain parental consent to processing. Privacy policies for such sites should be in language which children can understand so should not be overly legalistic or complex. Websites might adapt the information provided to suit children where necessary by first asking site visitors to confirm they are over 18, for instance, as is common practice on websites for gambling or alcoholic drinks.

In view of historic practice, each of a business' various databases may have differing levels of consent from the relevant data subject; harmonising these consents will need to be managed with care.

Accountability

The GDPR introduces the concept of "accountability" under which data controllers must:

- assess the risk that their processing poses to data subjects;

- carry out data protection impact assessments and keep enhanced records; and
- be able to demonstrate that they have appropriate technical and organisational measures in place to ensure that their processing is compliant (i.e. it is not enough to demonstrate that no breach has occurred). The appropriate measures to implement are left to each data controller to decide depending on the nature and size of its business and the risks posed by its processing.

Privacy by design

The GDPR introduces a concept of "privacy by design" to encourage businesses to make data privacy endemic in their organisation. Data controllers must:

- integrate safeguards into their processing systems both at the time of deciding the means of processing and also whilst that processing is taking place;
- regularly consider updating their security/processes to reflect developments in technology (n.b. the cost of implementing such technology can be balanced against the risks to the rights of the individuals posed by the processing);
- consider "pseudonymisation" of personal data to ensure that data cannot be attributed to a specific individual without additional information (e.g. referring to customers using an ID number as opposed to their name);
- institute "data minimisation" measures, whereby data controllers only keep personal data which is "*adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed*" (in other words, collect and keep as little data as possible); and
- carry out an "impact assessment" before introducing new processing methods to assess the risk posed to personal data. Such assessments will be mandatory for: (i) large-scale processing of sensitive personal data (e.g. a transfer of medical records); or (ii) any systematic automated analysis/decision making (including profiling) which will significantly affect the individuals concerned (e.g. an automated credit check). If the new activity is high risk, businesses must seek the regulator's view on whether it complies with the GDPR.

***Action** – Due to the introduction of the concepts of "accountability" and "privacy by design", organisations must:*

- *delete (or take steps equivalent to removing access to) data regularly which they no longer need. This has the added advantage of reducing the scale of data loss should there be a security breach. If data is not being used, then why risk losing it and the consequences of doing so?*
- *take privacy and security into account from the inception of a new product, embed these concepts into all systems and processes and monitor compliance on an on-going basis. Computer systems might be designed to minimise the amount of data that is stored or to automatically audit that data to identify inactive customers (whose data it is unnecessary to retain); and*
- *ensure that staff training is in place to help them handle data correctly and to respond to incidents of data loss or data breaches.*

Data protection officers

If a data controller or processor regularly processes sensitive personal data on a large scale they must appoint a data protection officer to ensure that data subjects' rights are safeguarded.

Action *– Businesses should consider the data they are processing (i.e. is it sensitive) and whether they are therefore obliged to appoint a data protection officer. Regardless of whether a business is obliged to appoint a data protection officer, such an appointment would be advisable in any event to ensure that the risk of data loss and cyber security breaches are monitored and minimised (this is particularly important for businesses which process large amounts of data). Businesses may find it helpful to have an individual responsible for evaluating these risks on an ongoing basis who can then develop and implement policies to deal with these threats and stress test the current systems.*

Enlarged definition of "personal data"

The GDPR expands the definition of personal data and clarifies that this can include information that can identify a person: (i) online, for instance by the use of cookies and IP addresses; and (ii) by reference to their physical, physiological, genetic, mental, economic, cultural or social identity.

Records

Data controllers will no longer be required to register with the authorities prior to commencing processing; instead, they must keep records of their processing activities available for inspection.

Action *– In order to be able to demonstrate compliance, businesses should now be conducting an audit to determine (and record):*

- *What types of personal data the business holds. Even small businesses are likely to hold multiple types of personal data, e.g. customer/employee/suppliers' contact and bank details; employment records. Larger or more complex businesses might hold personal data such as online identifiers (e.g. cookies) and biometric records (e.g. data used for facial, eye and finger print recognition).*
- *Where this personal data is stored. For example, customer contact details might be stored in a web/cloud based system, an electronic contact database or even old-fashioned hard copy address books.*
- *Where this personal data comes from. For example, was it collected from customers upon entry into a commercial relationship, during a transaction, upon the provision of services, or was it bought from a third party database or mined from publicly available sources?*
- *How this personal data is used/ processed. For example, is it used for marketing/profiling or employment purposes?*
- *In relation to each type of processing, what the legal justification for retaining and processing the data is. For example, has the customer consented to processing in this manner (and what record does the business have to evidence this)? Is the processing necessary for the legitimate interests of the data controller (and if so, why is this considered to be the case)?*

Once the business has conducted this 'baseline' audit, it should put procedures in place to keep its records current and take account of any new forms of processing which are introduced. Using the results of this audit, businesses should also explain in their privacy policies how they intend to process their customers' personal data and what their justification for this processing is.

Profiling

The GDPR tightens restrictions on profiling (collating information about a person from a wide range of sources to build up a valuable matrix of data e.g. data on a consumer's habits so as to produce targeted advertising). Profiling includes any analysis or prediction of a person's location or movements. Individuals have the right not to be subject to a decision based solely on automated processing unless the:

- individual has given explicit consent;
- profiling is necessary for the performance of a contract between the individual and the data controller; or
- profiling is authorised by the law of the data controller's country (subject to the individual's rights, freedoms and legitimate interests being safeguarded).

***Action** – If a business uses "profiling" (i.e. automated processing to aid decision making) it must allow individuals to: (i) request human intervention in this process; and (ii) express their view and contest any decision based upon the outcome of such profiling.*

Data processors

Data processors are now jointly liable with data controllers for any damage caused by a breach of the GDPR and must:

- notify data controllers when engaging further processors;
- ensure their contracts adequately allocate risk between the controller and them;
- implement appropriate technical and organisational measures to safeguard personal data; and
- notify data controllers of any data breaches.

***Action** – Data controllers should review/ amend their contracts with data processors to ensure the processor's obligations comply with the GDPR. Data processors (e.g. cloud service providers) should carefully audit their businesses to ensure they have adequate security and technological measures in place (and otherwise comply with the GDPR). In particular, data processors should ensure that they have procedures in place to report data breaches to the data controllers for whom they work.*

Territorial scope

The GDPR now catches data controllers and processors outside the EU/EEA if they: (i) offer goods or services to EU/EEA data subjects (irrespective of whether payment is required); or (ii) monitor EU/EEA data subjects' behaviour (as far as that behaviour takes place in the EU/EEA). This is likely to capture businesses which: (i) advertise goods or services online in the language or currency of a member state; or (ii) track consumer activities or target marketing at consumers within the EU/EEA.

***Action** – Non-EU businesses should evaluate whether they will be caught by the GDPR and, if so, act immediately to prepare for compliance. If the business has not previously had to comply with data protection regimes, it may take some time to bring its procedures into line.*

International transfers

Explicit consent, Model Clauses and Binding Corporate Rules (BCRs) will continue to act as the principal routes to enable international transfers of data:

- Consent – Due to tightened rules on consent, data controllers will need to consider whether data subjects have been sufficiently informed of the risks of international transfers.
- Model Clauses are the standard contractual clauses approved by the European Commission and will remain the most commonly used method to ensure compliance with international transfer requirements.
- BCRs are rules formulated by data controllers to govern how/when personal data can be transferred to affiliates located outside of the EU. BCRs must be submitted to the data controller's lead data protection authority for approval (the lead authority will also seek approval from any other relevant authorities). Once approved, BCRs allow data controllers to make (intra-group) transfers of personal data to affiliates outside the EU. The approval of BCRs should be more streamlined in future.

Foreign court orders

A foreign court order will only justify an international transfer of data if there is a treaty in force between the countries which provides for the mutual recognition and enforcement of judgments.

Data breach notification

If there is an accidental or unlawful destruction, loss, alteration or unauthorised disclosure of data and this is likely to result in a:

- "Risk" to the rights and freedoms of individuals, then the data controller must notify the data protection authority of this breach without undue delay (where feasible and appropriate, within 72 hours of becoming aware of it). They must explain what happened, specify the number of individuals affected and how they intend to rectify the breach.
- "High risk" to the rights and freedoms of individuals (e.g. discrimination, identity theft, financial loss, reputational damage, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage), then the data subject must be notified of the breach without undue delay.

No notification will be required if there is no risk (e.g. because the data was encrypted), however records must be kept even if no notification is required.

***Action** – Data controllers should ensure that policies exist (and staff are adequately trained) to identify and report any data breach quickly (if possible within 72 hours of becoming aware of it). Where notification cannot take place within 72 hours, the data controller should be prepared to explain the delay. As part of the audit mentioned above, organisations could categorise the data they hold to determine whether loss of that data would require notification (e.g. to evaluate the risk it poses) and speed up the process of notification should a data breach occur.*

Data controllers should encrypt personal data, where feasible and proportionate to do so, so that any data loss will be low risk (and will not require notification).

It is important to respond quickly and effectively to data loss as a business' response can mitigate or aggravate the damage to its reputation following the loss.

Companies should think about having internal or external personnel perform penetration tests against their current systems to identify security weaknesses and to understand how they are vulnerable to cyber attacks.

Fines

Data controllers and processors could be fined up to **€20m or 4 per cent of their worldwide annual turnover (whichever is higher)** for non-compliance with the GDPR. Organisations can be fined for both data breaches and failures to report breaches.

***Action** – Businesses will need to give far greater weight to data protection compliance than has previously been the case. The cost of such compliance is likely to be easily justified when compared against the potential fines and reputational damage which could be caused by a breach.*

Right to be forgotten

Unless a data controller has legal or legitimate grounds to continue processing data, it must erase personal data if: (i) the data subject objects to the processing or withdraws their consent; or (ii) the data is no longer necessary for the purposes for which it was collected. This codifies and expands the "right to be forgotten" recognised by the CJEU in the "Google Spain" case (the right for a data subject to be removed from search engine results if the link is "inadequate", "irrelevant" or "excessive").

***Action** – Businesses should formulate policies and procedures to enable individuals to exercise their "right to be forgotten" and withdraw their consent to processing. Alongside this, businesses must produce guidance for staff as to when data can be retained (despite the objections of the data subject). Equally, businesses should put systems in place which will identify dormant data or inactive customers. This form of "data audit" will help companies to identify data which is no longer necessary. Deleting dormant data has the added benefit of reducing the scale of any data loss.*

Enhanced subject access requests

Data subjects will have a right to obtain copies of their personal data in a commonly used and machine readable format (at present, hard copies will suffice). This data must be provided free of charge and within one month (at present a small fee can be charged and the time limit is 40 days).

However, data controllers will now have the right to refuse the request or charge a reasonable fee if the request is "manifestly excessive" (i.e. it would take a team of people days to prepare).

Data subjects also have the right to request that inaccurate data is corrected.

***Action** – Businesses should bolster their technological and human resources to facilitate compliance with more onerous subject access obligations i.e. the shortened timescales for responding and the requirement to provide personal data (including online identifiers) on request in an electronic and commonly used format. Given that data subjects will no longer have to pay (in most circumstances), the volume of subject access requests may increase significantly.*

CONTACT DETAILS

If you would like further information or specific advice please contact:

GEOFF STEWARD
PARTNER
LITIGATION AND DISPUTE RESOLUTION
DD+44 (0)20 7849 2341
geoff.steward@macfarlanes.com

RUPERT CASEY
PARTNER
COMMERCIAL
DD+44 (0)20 7849 2256
rupert.casey@macfarlanes.com