HUNTON& WILLIAMS

Hunton & Williams'

Executive Briefing Paper
Proposed General Data Protection Regulation

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Hunton & Williams
30 St Mary Axe
London
EC3A 8EP
United Kingdom

Table of Contents

HUNTON& WILLIAMS

Executive Briefing Paper

Proposed General Data Protection Regulation

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Hunton & Williams
30 St Mary Axe
London
EC3A 8EP
United Kingdom

Introduction

On 25 January 2012, the European Commission (the "**Commission")** released its widely anticipated data protection legislative framework proposal, intended to replace Directive 95/46/EC (the "**General Directive**"). The Commission's proposal consists of two instruments: *a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (the "**Draft Regulation**") and *a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* (the "**Draft Directive**"). Copies are available on the Commission's website at

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf and
http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf respectively.

The Draft Regulation will have a significant impact on business. In particular, businesses will need to increase the resources they dedicate to data protection and privacy compliance. The Draft Regulation contains many prescriptive requirements, including the need to employ dedicated privacy personnel, and to maintain detailed policies and documentation evidencing a comprehensive data privacy compliance programme. These requirements are supported by tougher penalties, including the possibility of fines of up to 2% of a company's worldwide turnover.

Such strict requirements and significant fines mean that organisations must start to consider how the changes may affect their activities and plan ahead. Failure to do so could mean that organisations are left with new requirements to implement, without having set aside appropriate resources.

Hunton & Williams has produced this Executive Briefing Paper to assist you in identifying key changes in the Draft Regulation which are likely to have a significant impact on your business.

This Executive Briefing Paper is divided into nine sections covering:

1. Definitions
2. Scope
3. Data quality principles
4. Overseas transfers
5. Security
6. Supervisory authorities
7. Internal controls
8. Individual rights
9. Exemptions

Each section consists of:

A. An explanation of the relevant provisions;
B. A short explanation of how the Proposed Regulation differs from the General Directive; and
C. A short commentary.

Frequently Asked Questions

What will happen to the General Directive? How is a regulation different?

As matters currently stand, the General Directive will be repealed and replaced by the Draft Regulation and Draft Directive. Unlike a directive, a regulation is directly applicable law and does not require implementation by individual Member States. If the current proposals come to fruition, existing data protection laws across the EU will be replaced by one regulation. The data protection regimes across the EU will take a significant step closer to harmonisation, although some national differences will remain, for example, in relation to court procedures, exemptions and potentially in the treatment of health and employment data. The Draft Directive will only apply to personal data used for criminal justice purposes, such as policing. It will be left to Member States to implement the Draft Directive which will, inevitably, lead to some variation across Member States.

Who will be affected by these changes?

The Draft Directive will only apply to public authorities which deal with personal data relating to criminal offences and prosecutions when they are processing personal data for those purposes. All other processing of personal data will be covered by the Draft Regulation. The Draft Directive, while very important, is therefore not relevant to most data controllers. This Executive Briefing covers the Draft Regulation only.

How will the Draft Regulation and Draft Directive become law?

Both the Draft Regulation and Draft Directive will be considered by the European Parliament, the Commission and the Council of Ministers. The Government of each Member State will take part in Working Groups, discussions and lobbying activities over the next two years. There will be Working Groups at officer level and at a political level in the Council. The Parliament will review the drafts and propose amendments which will be considered by the Commission and eventually the Council, with a view to reaching agreement. If, after a number of reviews and discussions, it is not possible to reach agreement between the Parliament, Commission and Council, matters will be decided by a Conciliation Committee. A Conciliation Committee is made up of representatives from the Parliament and the Council (although members of the Commission will also be present) with the aim of reconciling differences between the two bodies.

Will there be changes to the current drafts?

Yes, there will be changes. There is no doubt that the current drafts will alter as they are reviewed by the Parliament, the Commission and the Council. The final form of the Draft Regulation and Draft Directive will become clearer as they move through the legislative process. The Draft Regulation and Draft Directive should not be regarded as settled, although the main themes are unlikely to change. Organisations should be cautious about making detailed changes to practices or policies at this stage but it is important to begin to evaluate how the changes will impact your organisation and how you should be preparing for those changes.

What is the timescale?

Navigation of the political process is expected to take approximately 18 months from the release of the current Draft Regulation and Draft Directive. There will then be a further period before the instruments are implemented in Member States. The earliest effective date for a change in the law, based on the current drafts, is expected to be around 2016.

Section 1 - Definitions

There are several new or amended defined terms in the Draft Regulation. Some of the more significant changes are considered below.

- The definition of **data subject** now incorporates the definition of personal data and has been expanded to include location data and on-line identifiers in the list of factors which may lead to an individual being "identified or identifiable".
- The definition of **consent** has been tightened and any consent must be explicit.
- A definition of a **child** has been introduced and means any person under 18 years of age.
- **Joint controller** has been defined and there is an obligation on joint controllers to establish their respective responsibilities for compliance between themselves.
- **Genetic data** has been defined and is one of the special categories of personal data afforded additional protection under the Draft Regulation.

Personal data: The definition of personal data has been amended and shortened to "any information which relates to a data subject" (Article 4(2)). There is no extension to the coverage of manual data.

Data subject: Under Article 4(1), the definition of a data subject has been expanded and now contains the previous definition of "personal data". It also includes location data and on-line identifiers among the list of factors which may lead to an individual being "identified or identifiable". The definition clearly takes into account the growth of online activity since the drafting of the General Directive.

Consent: Under Article 4(8), the definition of consent has been amended. Data subject consent is defined as any "freely given, specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or clear affirmative action, signifies agreement to personal data relating to them being processed". In addition, the following requirements apply to consent:

- The controller bears the burden of proof for the data subject's consent;
- Where written consent relates to more than one matter, consent must be "separate and distinguishable in appearance from the other matter";
- Consent may be withdrawn at any time;
- Consent will not be valid as a legal basis "where is a significant imbalance between the position of the data subject and the controller".

Child: A new definition is contained in Article 4(18) of the Draft Regulation. A child is defined as anyone under 18 years old, although the substantive rules in the Draft Regulation apply to a child below 13 years of age. Under Article 8(1), the processing of personal data in the context of providing information society services to a child under 13 is lawful only with the consent of the child's parent or custodian.

Genetic data: This category of personal data has been added to the definition of special categories of personal data. Genetic data is defined in Article 4(10) as any data which relate to the characteristics of an individual which are inherited or acquired during early prenatal development. Under Article 9(1) of the Draft Regulation, as a special category of personal data, genetic data are afforded additional protection and a controller wishing to process genetic data will have to meet one of the conditions for processing such data.

Differences from the present position

Under the General Directive explicit consent is only required to legitimise the processing of sensitive personal data; under the Draft Regulation explicit consent must be obtained for the processing of all types of personal data. The new requirement for all consent to be explicit will require a higher standard of consent from data subjects. This, combined with the fact that the controller will bear the burden of proof to demonstrate that it has obtained valid consent, indicates a more conservative approach to the use of consent generally. The remaining provisions concerning consent in the Draft Regulation appear to confirm current understanding and practices. For example, it is accepted that a data subject has the right to withdraw his or her consent at any time.

The expanded definition of data subject appears to broaden the scope of data considered to be personal data and therefore subject to the Draft Regulation. The specific inclusion of location data and online identifiers explicitly raise the issue of how far such data (e.g., IP addresses) act as identifiers.

The introduction of a specific provision relating to any personal data processed in the context of offering an information society service to a child under 13 should be noted. The provision has been included to address problems raised by children's use of the internet.

Commentary and Actions

The strengthening of the provisions governing consent could prove challenging for organisations which rely on it for processing personal data. Businesses will need to consider how to incorporate the requirements for obtaining valid consent into their practices. Where "box ticking" is used to evidence explicit consent, there is a risk that this may negatively impact individuals' experiences by increasing the number and complexity of statements to be filled out or buttons to click. In addition, while the provisions relating to consent appear designed to protect individuals, they raise questions as to the effectiveness of explicit consent obtained from individuals. In practice, if given a choice, most individuals tend not to tick boxes or read the accompanying text, even when asked to confirm that they have done so. Thus the requirement for consent to be explicit may do little, in practice, to protect individuals. Whether consent can be made more meaningful with the addition of the new provisions is doubtful, given the challenging nature of consent.

The introduction of the requirement to obtain parental consent for personal data relating to a child under 13 processed in the context of offering an information society service has several practical difficulties. In particular, it is not clear how and at what point parental consent can, and should, be obtained. As the UK Information Commissioner ("ICO") has noted in his initial analysis of the Draft Regulation, such a requirement does not take into account circumstances in which children under 13 may wish to access services without parental consent, such as a confidential support line. Article 8(1) does not allow for such situations.

- Review any consent language currently used for data collection to ensure that it is explicit and indicates affirmative agreement from the data subject.
- Where children's personal data are processed in the context of offering information society services, consider mechanisms to obtain parental consent for this processing.

Section 2 - Scope of the Draft Regulation

The Draft Regulation will apply to all controllers which are established in the EU and process personal data in the context of that establishment in the EU. It will also apply to controllers outside the EU which process personal data in order to offer goods or services to data subjects who are resident in the EU or monitor the behaviour of data subjects resident in the EU. Data processors which are established in the EU will also be directly subject to the Draft Regulation; those which are not established in the EU do not appear to be covered.

For organisations with more than one establishment in the EU, the Draft Regulation introduces the concept of a 'main establishment'. The location of the main establishment will determine which lead supervisory authority will deal with an organisation, as the supervisory authority local to the place of the main establishment will be responsible for supervising the organisation. The main establishment of a controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative (subject to certain exceptions) to act on behalf of the controller and deal with supervisory authorities.

The territorial scope of the Draft Regulation is set out in Article 3(2). It brings businesses which have no physical presence in the EU but which conduct activities offering goods or services to EU data subjects, or monitoring their behaviour, within the scope of the Draft Regulation. Although there is no definition of the concept of monitoring behaviour in the Draft Regulation, the recitals imply that this occurs where individuals are tracked on the internet with data processing techniques that consist of applying a "profile" to an individual in order to make decisions concerning the individual or for analysing or predicting an individual's personal preferences, behaviours and attitudes. It seems, therefore, that behavioural advertising could be covered by this description.

Article 4 of the Draft Regulation introduces the concept of a main establishment. An organisation's main establishment is the place of its establishment in the EU where the main decisions as to the purposes, conditions and means of the processing of personal data are taken. If no control is exercised over the processing in the EU, but processing activities are carried out in the context of an establishment in the EU, that establishment is the main establishment. In determining where the main decisions as to the purposes, conditions and means of processing are made, the effective and real exercise of management is the decisive factor.

Under Article 25(1) of the Draft Regulation, if the controller is based outside the EU, it has an obligation to appoint a representative (subject to certain exceptions). The representative acts on behalf of the controller and can be addressed by any supervisory authority. Supervisory authorities are not under any obligation to deal with the representative and can deal directly with the controller instead. The controller can decide where the representative will be located, as long as it is in a jurisdiction in which the controller operates.

Differences from the present position

The Draft Regulation will extend the number of businesses affected by EU data protection legislation; not only will business based in the EU be subject to the Draft Regulation, but also businesses based outside the EU which either offer goods or services to European data subjects or monitor their behaviour. This a significant step to protect the personal data of EU data subjects, although one that may present practical difficulties. Non-EU businesses, particularly those which sell into several Member States, will be subject to the law of every Member State in which they operate. It is difficult to see how non-compliance by businesses outside the EU will be enforced.

The introduction of the requirement to appoint a representative in the EU if a controller is located outside the EU is also a significant step. It allows regulators to have a point of contact for liaising with the controller if they wish to do so, although there is no obligation for a supervisory authority to deal with the representative.

Commentary and Action

The test of main establishment has been criticised. Although it is intended to assist companies, it only applies where one legal entity operates through different offices or branches in the EU and not where there are different legal entities. The UK ICO has raised concern that the test of main establishment may mean that organisations which have decentralised decision making or which have decision making for different aspects of their processing located in different countries could be excluded from the benefit of having a lead supervisory authority.

- Organisations based outside the EU but which sell goods and services globally or monitor the behaviour of individuals globally need to consider whether the selling is targeted at EU residents and the monitoring of behaviour applies to EU residents.

- Organisations based outside the EU but within the scope of the Draft Regulation will need to appoint a representative. There is some flexibility in determining where the representative will be located. Consideration should be given to which European jurisdiction, out of those in which the business operates, is most appropriate.

- Organisations which are established in the EU, should consider whether they have separate legal entities or just one entity, where the organisation processes the majority of personal data, what each

branch does and where the organisation has most control over its processing operations. This will allow the organisation to determine the location of its main establishment.

Section 3 - Data Quality Principles

Main Obligations of Controllers and Processors

The Draft Regulation sets out principles relating to personal data processing which largely mirror the principles under the General Directive. Essentially, the principles set out the manner in which personal data should be processed. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. Personal data must only be collected for specific purposes and be limited to the minimum necessary to satisfy the processing purposes. The principles require that personal data are accurate, up to date and stored for no longer than is necessary for the purposes for which the personal data are processed.

The general obligations of the controller and processor are set out in Chapter IV of the Draft Regulation. Controllers will be obliged to adopt policies and take measures to ensure that the processing of personal data is performed in compliance with the Draft Regulation. The measures include maintaining documentation, implementing security requirements, performing data protection impact assessments ("**DPIAs**") and complying with requirements to notify or obtain approval from the relevant supervisory authority before undertaking specified types of processing.

Chapter II sets out the overarching principles relating to how personal data are to be processed. Article 5 of the Draft Regulation mirrors requirements in the General Directive. Processing should only occur if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data. Article 5(c) enshrines the concept of data minimisation and requires personal data to be adequate, relevant and limited to the minimum necessary in relation to the processing purposes. Article 5(b) requires personal data to be accurate and kept up to date, and that it meets data quality and retention requirements. Article 6 sets out the conditions to make the processing of personal data lawful, which again largely mirror the grounds in the General Directive.

The principle of accountability is set out in Article 5(f) and requires that personal data are processed under the responsibility and liability of the controller, which is also responsible for compliance with the Draft Regulation. Other provisions in the Draft Regulation implicitly establish a degree of shared responsibility with the data processor, such as Articles 33 and 34 on prior authorisation. There are no specific provisions to explain how these shared responsibilities are to be exercised, or how related disputes should be resolved.

Chapter IV of the Draft Regulation imposes duties of responsibility and accountability on data controllers. Under Article 22(1) of the Draft Regulation, controllers shall adopt policies and implement appropriate measures to ensure and demonstrate that the processing of personal data is performed in compliance with the Draft Regulation. The measures to be implemented, listed under Article 22(2), imply the criteria against which accountability of the controller will be assessed. Controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs, comply with requirements for prior notification or approval from the relevant data protection authority and designate a data protection officer, if required. The Commission may adopt delegated acts for the purpose of specifying any further criteria and requirements for the measures referred to in Article 22(1).

Data processors' responsibilities have been significantly expanded from the existing General Directive. Article 26(1) requires controllers to 'choose a processor providing sufficient guarantees of security'. Article 26(2) imposes an obligation on both parties to enter into a contract or other legal act covering the obligations of the parties. Both parties also have direct obligations for implementing appropriate technical and organisational measures. Processors may be ordered by the supervisory authority to comply with data subjects' requests to exercise their rights, even though the primary responsibility for such compliance rests with the data controller.

Differences from the present position

Article 5 of the Draft Regulation strengthens the general conditions for processing by imposing specific limitations on data processing. Articles 5(c) and (e) make explicit reference to data minimisation, a concept which was only implicitly included in the General Directive. Organisations that process personal data will have to monitor and limit the amount of data they process and retain. Under the General Directive, controllers are obliged to ensure that the principles are complied with. The Draft Regulation imposes a more explicit obligation on controllers, requiring that personal data be processed under the responsibility and liability of the controller. In addition, controllers must ensure and demonstrate, for each processing operation, compliance with the Draft Regulation.

The Draft Regulation introduces direct obligations on processors. This is significantly different from the present position in which only limited statutory obligations are imposed on processors, and most obligations emanate from their contractual relationship with the controller.

Commentary and Actions

The data processing principles contained in Article 5 of the proposed Draft Regulation are an expansion of the existing principles. The explicit reference to data minimisation is significant and will require practical changes in the way in which organisations collect and process personal data.

The introduction of an explicit principle for data to be processed under the responsibility and liability of the processor is a major change. Processor responsibility is not a new concept but under the General Directive it is limited to security obligations and those obligations which are imposed on the processor through a contract. There is some ambiguity in the provisions of the Draft Regulation as to the extent to which compliance responsibility will lie with the processor as well as the controller. This could lead to difficulties for controllers and processors who may be unclear as to where their respective responsibilities begin and end.

- Data controllers will need to consider the logistics and the process for monitoring and limiting the amount of data they process and retain. A more rigorous approach to data retention and erasure is likely to be required.

- Data processors will need to review their new processing obligations and ensure that these are understood and can be satisfied.

Section 4 - Overseas Transfers

The Draft Regulation does not propose significant changes in relation to overseas transfers. The basic rule remains that the transfer of personal data from the EEA is prohibited unless one or more of the safeguards or derogations apply. The Commission may make a finding that the protection offered to personal data in a country outside the EEA is adequate. It can also make such findings in relation to particular international organisations or a territory or processing sector within a third country. The Commission may approve model contractual clauses under which personal data can be sent to a country which is not considered adequate. The current approved model contractual clauses will remain in force. Supervisory authorities may also approve model contractual clauses, subject to the clauses having been accepted by the European Data Protection Board under the consistency procedure. Binding Corporate Rules ("BCRs") are formally recognised. The provisions set out for BCRs largely follow the Article 29 Working Party Opinions on BCRs and current practice. BCRs are also made applicable to data processors.

A new derogation is introduced where the data transfer is necessary or is undertaken for the purposes of the legitimate interests of the controller or processor and the transfers are neither "frequent" nor "massive". In a significant change for the UK, this will be the only circumstance in which controllers are able to make their own determination of adequacy.

Where controllers and processors rely on BCRs or approved model contractual clauses (whether Commission or supervisory authority approved), no further authorisations (such as permits) are required for transfers to take place. Non-standard model contractual clauses require approval from the local supervisory authority. Further, there is no provision for controllers and processors to make their own adequacy findings (as controllers may currently do in the UK) apart from under the new derogation. Under Chapter V of the Draft Regulation, transfers of personal data to third countries or international organisations (including onward transfers from one third country or international organisation to another) are prohibited unless: (i) there is a Commission adequacy finding; (ii) the controller or processor has adduced appropriate safeguards; or (iii) the controller or processor can rely on a derogation.

Commission adequacy findings may relate to an international organisation, third country, or a particular territory or processing sector within a third country (Article 41).

Article 42 sets out four, non-exhaustive, appropriate safeguards: (i) BCRs; (ii) model contractual clauses adopted by the Commission; (iii) model contractual clauses adopted by a supervisory authority in accordance with the consistency mechanism; and (iv) individual contractual clauses authorised by the supervisory authority. Where controllers and processors rely on BCRs or Commission (or supervisory authority) adopted model contractual clauses, no further authorisations (such as permits) are required for the transfers to take place.

Article 43 sets out the provisions for BCRs. BCRs can now be adopted by processors; however, it is not clear whether an organisation could enter into one set of BCRs as both a controller and a processor. BCRs apply to groups of companies and cannot be extended to cover non-affiliates. The rules require that they are made legally binding on all the companies in the group, give enforceable rights to data subjects and are supported by the full documentation and procedures set out in Article 43. The requirements largely follow the Article 29 Working Party Opinions and current practice. In addition, the approval of BCRs is subject to the consistency procedure; they cannot be agreed by a single regulator. There are no provisions in the Draft Regulation which streamline the procedure for approval of the BCRs.

Where no adequacy decision exists and appropriate safeguards have not been adduced, Article 43 sets out eight permitted derogations:

i) informed consent;
ii) necessary for the performance of a contract between the data subject and the controller, or pre-contractual steps taken at the data subject's request;
iii) necessary for the conclusion or performance of a contract between the controller and a third party, concluded in the data subject's interest;
iv) necessary on important public interest grounds;
v) necessary for the establishment, exercise or defence of legal claims;
vi) necessary to protect the vital interests of the data subject or of another person, where the data subject is incapable of giving consent;
vii) the transfer is made from a public register; or
viii) necessary for the purposes of the legitimate interests pursued by the controller or processor which cannot be qualified as frequent or massive, and the controller or processor has assessed the transfer and adduced appropriate safeguards, where necessary.

The derogations reflect those permitted under the General Directive, with the addition of a new derogation that the transfer is necessary for the purposes of the legitimate interests pursued by the controller or processor, as long as the transfers are infrequent and not massive.

Differences from the present position

The Draft Regulation does not significantly alter the mechanisms which are available to deal with overseas transfers. As is currently the case, transfers to third countries are not permitted unless: (i) an adequacy finding exists; (ii) appropriate safeguards have been adduced; or (iii) a derogation exists.

An explicit general prohibition on overseas transfers to international organisations as well as to third countries is introduced which is mirrored by a provision allowing the Commission to make adequacy findings in relation

to such organisations. The Commission may make adequacy findings for third countries (as is currently the case) as well as for specific territories or processing sectors within a third country.

BCRs are formally recognised under the Draft Regulation and are extended to data processors. The provisions largely follow current practice and, as such, the procedure to obtain approval for BCRs is unlikely to change significantly. In addition to Commission approved model contractual clauses, individual supervisory authorities may adopt model contractual clauses, although these are subject to the consistency mechanism. Where overseas transfers are made subject to BCRs or Commission (or supervisory authority) approved model contractual clauses, supervisory authorities may no longer require further authorisations, such as permits, for the transfers to take place.

Data controllers will no longer be able to make their own determination as to the adequacy of protection in a third country. Currently, this is an acceptable mechanism for international transfers in the UK, although not in other EU countries. However there is a new derogation which applies where a transfer is necessary for the purposes of the legitimate interests of the controller or processor, but the transfer is not massive or frequent.

Commentary and Actions

The power of the Commission to make adequacy findings in respect of particular international organisations, territories or processing sectors, as well as in relation to third countries is likely to be welcomed as pragmatic, and may be welcomed particularly by large-scale data processors with operations in the U.S. or other third countries, such as India or the Philippines. This provision seems unlikely to change during the legislative process.

The Draft Regulation formally recognises BCRs as an appropriate safeguard, and permits their use by processors as well as controllers. These changes are likely to be generally welcomed and seem unlikely to change during the legislative process, although there will be concern that all BCRs will require approval through the consistency procedure.

Similarly, the ability of supervisory authorities to adopt model contractual clauses, in addition to the Commission, is likely to be welcomed, as will the use of approved model contractual clauses without the need for further authorisations. Currently, many supervisory authorities require prior notification or approval for overseas transfers, even where the controller utilises model contractual clauses. This simplification is therefore likely to be welcomed.

Contractual clauses individually negotiated with data recipients will require prior authorisation from the supervisory authority. This introduces a higher burden on both controllers and processors, as well as supervisory authorities, than under the existing rules in some Member States. For example, in the UK, controllers may make their own adequacy findings and use contractual clauses without prior approval. Such a change will result in some loss of flexibility for organisations.

It is not entirely clear from the Draft Regulation how the newly introduced derogation which permits transfers made for the purposes of the legitimate interests where they are not “frequent” or “massive” will work in practice. It is difficult to see how these conditions on the transfer of personal data offer any additional protection. As long as a transfer is made on a legitimate basis and the personal data are appropriately safeguarded, it seems unnecessary to focus on the regularity of the transfer or the quantity of data transferred.

- Organisations which have an embedded privacy programme should start to consider whether their organisation is suitable and ready for BCRs as a mechanism for its international transfers.

- UK based organisations which currently rely on adequacy determinations for transfers of data will need to consider model contractual clauses for any future transfers of data.

Section 5 - Security and Breach Notification

Chapter IV, section 2 of the Draft Regulation deals with data security and breach notification obligations. The Draft Regulation introduces security obligations which expand on the security obligations imposed under the General Directive. Under Article 30(1), both the controller and processor are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the processing risks and the nature of the personal data to be protected. Article 30(2) requires both parties to evaluate the processing risks and implement measures to protect against accidental, or unlawful, destruction or loss of data. Data should also be protected against unauthorised processing, including unauthorised disclosure, dissemination, access or alteration of personal data.

The Commission has the power, under Article 30(3), to adopt delegated acts to further specify the criteria and conditions for the technical and organisational measures to be implemented. These may include determinations of the meaning of 'state of the art', with regard to specific industry sectors, specific processing situations and developments in technology. Additionally, under Article 30(4), the Commission may adopt implementing acts to explain the requirements for protecting data against unauthorised processing and verifying the lawfulness of the processing.

Article 31 introduces a mandatory breach notification requirement for all controllers, regardless of the sector in which they operate. This provision builds on the breach notification requirements implemented under e-Privacy Directive. Controllers are required to notify the data protection authority 'without undue delay' and, where feasible, within 24 hours of becoming aware of the data breach. Controllers which notify after this 24 hour period must justify the delay to the supervisory authority.

Article 31(3) sets out the details that should be notified to the supervisory authority including:

- the nature of the breach;
- categories and number of data subjects;
- details of the data protection officer; and
- measures taken to mitigate the adverse effects of the breach and consequences of the breach.

The processor is also under a duty to notify the data controller immediately if it becomes aware of a personal data breach.

Under Article 32, where a personal data breach is likely to adversely affect a data subject, either because their privacy or the protection of their personal data will be affected, the controller is required to communicate the breach to the affected data subject. Any communication to the data subject is to be made after the supervisory authority has been notified. The supervisory authority has the power to require a controller to notify an affected data subject if the controller has not yet done so. A limited exception to the duty to communicate the breach applies under Article 32(3) where a controller can demonstrate that it implemented measures which rendered the data unintelligible to anyone without authorised access, i.e., encryption of data.

Differences from the present position

The security provisions in the Draft Regulation largely mirror the existing rules found under Article 17 of the General Directive. The security of processing obligations have been expanded under the Draft to include processors as well as controllers. In addition, the Commission will, as a result of Article 30(3), be granted the power to adopt acts that further specify the 'criteria and conditions' for the technical and organisational measures to be implemented by both controllers and processors.

The Draft Regulation will significantly alter breach notification obligations. At present, under the General Directive, there is no mandatory breach notification requirement, although some countries, such as Germany, have their own personal data breach notifications laws. In other countries, such as the UK, notification of data breaches is recommended as best practice. Under Article 31 of the Draft Regulation, the controller will be under a duty to notify the relevant supervisory authority in the case of any personal data breach. The notification provision is prescriptive and Article 31(3) lists the type of information that should be provided by the controller when notification is made. The Draft Regulation also introduces a duty on the controller, under

Article 32, to notify personal data breaches to affected data subjects if the breach is likely to adversely affect the protection of their personal data or privacy.

Commentary and Actions

As the Draft Regulation does not significantly alter the position in relation to the security of processing, these changes have not been controversial. Although Article 30 extends the security provisions to processors, the substantive requirements are general in nature. It is likely that organisations will already have established measures, based on appropriate levels of security with regard to processing risks. Article 30 of the Draft Regulation reinforces the process for determining the level of security to be implemented.

The Draft Regulation significantly alters the position with regard to breach notification. Organisations and supervisory authorities have broadly welcomed the breach notification obligations but are concerned by the prescriptive requirements. The Draft Regulation sets out the timeframe within which breaches should be notified, as well as the details that must be notified. It fails, however, to specify the criteria for deciding what constitutes a data breach and there is no "de minimis" provision. There are concerns that supervisory authorities will be inundated by breach notifications, including minor breaches which are unlikely to cause harm, thereby slowing the supervisory authority's response to serious breaches.

The prescriptive nature of the requirement to communicate breaches to data subjects is problematic. Article 32 requires the controller first to notify a breach to the supervisory authority, and then to the affected data subjects. In instances where immediate notification to the data subject is recommended, for example when financial data has been disclosed, there is concern that imposing a sequence of notification is overly prescriptive and is an ineffective way to protect data subjects.

- Processors offering their services to controllers will be required by law to implement appropriate security measures. Processors should start to review their existing security provisions.

- Organisations should start to review existing contracts to ensure they include appropriate provisions relating to security, and consider whether any changes are likely to be required.

- Organisations from all sectors must consider adapting data processing functions and build in more effective ways of detecting breaches in order to comply with the introduction of breach notification requirements.

- Organisations should develop a strategy for dealing with personal data breaches that arise and should document this in a data breach response plan to be circulated throughout the organisation.

- Organisations should consider refreshing their training and awareness campaigns to include the identification of data breaches.

Section 6 - Powers of Supervisory Authorities and the Commission

There will be at least one separate supervisory authority in every Member State. In those Member States with a federal structure, such as Germany, there may be many supervisory authorities.

Each supervisory authority will oversee data controllers and data processors established in their jurisdiction. In broad terms this means that supervisory authorities will oversee all organisations with branches or places of business in their jurisdiction, and all public authorities. They will also oversee data controllers located outside the EU that offer remote services into the country but do not have a presence in the EU.

They will have wide powers to investigate and enforce. Investigation powers will include powers to require information and powers of entry and seizure, subject to judicial authorisation. Enforcement powers will include the right to order controllers and processors to take specific remedial actions, to suspend or ban processing (including data exports) and to order the erasure of data. Supervisory authorities will have powers

to impose fines for breaches of the Draft Regulation, up to a maximum of 2% of annual turnover for some breaches, although the Draft Regulation also states that sanctions must always be fair and proportionate.

Where businesses operate through separate companies or trade from outside the EU, they may be subject to the supervision of several supervisory authorities. In addition, data subjects in one country may complain about a data controller established in another country.

To address these overlaps there are rules dealing with the conduct of joint investigations. Most importantly, there will be a Board of all supervisory authorities chaired by the European Data Protection Supervisor ("EDPS"), which will have formal powers. Supervisory authorities will work together under the consistency mechanism to reach agreement on matters under their remit. If they fail to agree, the Commission has the power to resolve differences of opinion over enforcement matters. The Commission has an important role in producing detailed rules for implementing the Draft Regulation and in resolving disputes between supervisory authorities about the use of enforcement powers.

Chapter VI covers the role of the supervisory authorities. Supervisory authorities must be independent and must produce annual reports and information as well as exercising supervisory powers under Article 51(2). If one company operates in several EU countries then it can have a "home" or "lead" supervisory authority which is responsible for supervising all its activities. The lead supervisory authority must be the supervisory authority for the country in which the company has its main establishment. If personal data is processed in the context of other establishments, the lead supervisory authority has to apply the law of the country of the specific establishment. If there are differences over exemptions, for example, the supervisory authority will have to deal with those.

The consistency mechanism is the term given to the process by which supervisory authorities will work together to resolve differences of opinion on supervisory issues which affect data subjects in a number of Member States. It is set out in Chapter VII. The consistency mechanism described in Articles 57 to 63 involves stages in which draft measures and opinions are negotiated between the Board and the originating supervisory authority. There are no procedural safeguards on the face of the provisions for those affected; neither controllers nor processors, or data subjects who might be affected, have rights to be told of these exchanges, to have access to the opinions, to make representations or even to be heard. In the end, if the supervisory authorities cannot agree between themselves, the Commission can adopt a legal measure against which there is no judicial appeal or redress under Article 62.

The threshold for invoking the consistency procedure appears to be low. It is invoked, for example, where a supervisory authority wishes to take a "measure" against a business that operates in several countries, where a supervisory authority wishes to list a particular type of processing to be submitted for prior approval or to approve BCRs.

As well as powers to serve enforcement notices, supervisory authorities will be able to impose heavy fines for technical infringements under Article 79. In addition, they can insist on taking part in joint investigations in other counties and there are formal rules imposing obligations to cooperate to the extent, in the most extreme case, that one supervisory authority could take another to court for failing to take action that it wants to see taken against a controller or processor.

Chapter VIII sets out the individual remedies as well as sanctions. Articles 73 to 77 provide for individuals to have rights to take legal action for breach, including rights to compensation.

Differences from the present position

There are significant changes from the current position which appear to strengthen the powers of supervisory authorities. Much publicity has been given to the power to impose large fines but this should not obscure the other significant changes.

An action by a lead supervisory authority is likely to trigger the consistency mechanism. It appears to be easy for a supervisory authority to set the consistency process in motion. Once the consistency procedure is underway, it may be hard for those affected to follow proceedings.

As data processors will be directly subject to obligations under the Draft Regulation, they will also be subject to the powers of enforcement of the supervisory authorities.

Commentary and Actions

There have been expressions of concern about the absence of discretion in relation to fines and the potential level of fines.

There has also been concern about the exemptions from the obligation to appoint a representative.

The EDPS has commented on the consistency mechanism and the role of the Commission and suggested that supervisory authorities should be entitled to apply to the European Court of Justice against orders of the Commission.

Section 7 - Prior Notice to Supervisory Authorities and Internal Controls

The Draft Regulation introduces new obligations on data controllers and data processors. These include:

- Maintaining prescribed documentation;
- Mandatory Data Protection Impact Assessments ("DPIAs");
- Mandatory appointment of Data Protection Officers ("DPOs"); and
- Prior authorisation and consultation of supervisory authorities in some cases.

Data controllers and data processors must maintain documentation recording all their data processing activities. The documentation must be sufficiently detailed and organisations must ensure that they maintain information such as records of international data transfers, recipients of personal data and time periods for erasure of data.

DPIAs must be conducted prior to processing where the processing raises specific risks to the rights and freedoms of data subjects. Examples of processing which may present specific risks include processing sensitive personal data, profiling, processing that involves filings systems on children, genetic or biometric data and video surveillance data.

A data controller or data processor may consult a supervisory authority prior to the processing of personal data to ensure the proposed processing complies with the requirements of the Draft Regulation. In certain circumstances, a data controller or data processor may be required to obtain authorisation from a supervisory authority.

Article 28 requires that data controllers and data processors must maintain detailed documentation recording all their data processing activities. The documentation must contain at least the following information:

- the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
- the name and contact details of the DPO, if any;
- the purposes of the processing, including the legitimate interests pursued by the controller where this condition is being relied upon to legitimise the processing;
- a description of categories of data subjects and of the categories of personal data relating to them;
- the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for a legitimate interest pursued by them;
- the transfers of data to a third country or an international organisation, including the identification of that third country or international organisation; and
- a general indication of the time limits for erasure of the different categories of data.

This documentation requirement is intended to replace the current requirement for a data controller to notify its data processing activities to the relevant DPA. A data controller or processor must make the documentation available to a supervisory authority if requested.

A DPIA must be conducted prior to processing where the processing raises specific risks to the rights and freedoms of data subjects under Article 33. Examples of processing which may present specific risks include processing sensitive personal data, profiling, processing involving filing systems on children, genetic or biometric data and video surveillance data. Further, the supervisory authority may compile a list of processing activities which are to be subject to a mandatory DPIA and require prior consultation to the supervisory authority. Where a DPIA indicates there is a high degree of specific risk, the authorisation of the supervisory authority must be obtained under Article 34. A controller or processor may also voluntarily request the prior authorisation of the supervisory authority in relation to its proposed processing to verify compliance with the Draft Regulation.

A data controller or data processor with more than 250 employees or whose main activity involves systematic monitoring of individuals must appoint a DPO under Article 35. The DPO must be involved in all issues relating to the protection of personal data. The controller or the processor must designate a DPO for a period of at least two years, although the DPO may be reappointed for further terms. During their term of office, the DPO may not be dismissed, unless they no longer fulfil the conditions required for the performance of their duties. The DPO will be the point of contact for a supervisory authority and data subjects. The DPO must perform his/her duties and tasks independently of the organisation and must not receive any instructions regarding the exercise of his/her functions.

Differences from the present position

There are significant changes from the present position. First, the new requirements in the Draft Regulation apply to both data controllers and data processors. This extends the scope of obligations under legislation to data processors. While data processors may, in practice, be maintaining such documentation currently in order to comply with their contractual obligations to data controllers, the Draft Regulation requires this.

Second, while organisations are currently encouraged to complete DPIAs and organisations may voluntarily appoint DPOs, the Draft Regulation makes DPIAs and DPOs mandatory in certain circumstances. The requirement to appoint a DPO where an organisation has more than 250 employees, without any reference to the potential risk of processing, is in contrast to a more harms based approach.

Finally, the new requirements seek to introduce the concept of accountability in the Draft Regulation. Such a development is welcomed by many organisations. The prescriptive nature of the requirements, however, introduces a one size fits all approach to accountability, without taking into consideration the effect this may have on different types of organisations. For example, the requirement to maintain detailed documentation may be particularly onerous for SMEs. In addition, the requirement will be resource intensive as such information may quickly become outdated and will require constant updating.

Commentary and Actions

On the whole, the introduction of the new requirements is likely to increase the administrative burdens on organisations. In relation to the documentation requirements, the external obligation to register has been transformed into an internal obligation to maintain detailed documentation. The sheer amount of information to be documented will make this requirement onerous for organisations to comply with. This requirement will be particularly burdensome in countries that currently enjoy simplified notification systems, such as the UK. In addition, there are practical difficulties in maintaining such information when it is subject to alteration. Information is likely to become quickly outdated. Further, the requirement for both data controllers and data processors to maintain the required documentation may lead to duplication, resulting in multiple sets of paperwork documenting the same processing activities, and thus increasing costs.

The UK Commissioner has expressed doubt whether the requirement for policies and administrative measures to demonstrate compliance with the Draft Regulation will lead to effective accountability. The ICO acknowledges, however, that a failure to produce the required policies and administrative measures should be an aggravating factor when considering enforcement action to be taken against a data controller. There is a risk, however, that a supervisory authority will be required to take action against a controller whose processing

is fair and lawful, and does not negatively impact on an individual's privacy, merely because the controller does not have the necessary documentation in order.

In relation to DPIAs, while this is a useful process for organisations to undertake, there is a concern that if DPIAs become public-facing documents (as envisaged by the Draft Regulation) they may become tick-box exercises, rather than useful assessment tools, as data controllers seek to ensure that no sensitive or commercial information reaches the public domain. Similarly, the requirement to consult data subjects would be burdensome and it is not clear what the anticipated benefit of such a consultation might be. Data subjects may not have the requisite expertise or desire to fully understand and opine on data processing activities. Finally, there is also some concern that DPIAs would be required in too many instances and may apply to fairly routine processing activities, which many organisations undertake regularly.

In relation to DPOs, while their appointment may lead to benefits for some organisations, for others, DPOs are not appropriate. For example, some organisations may already have effective processes in place for ensuring data protection compliance and the introduction of a DPO would not necessarily add to this. The appointment of a DPO in circumstances where it is not appropriate is therefore an administrative burden rather than a helpful and strategic resource that is beneficial to an organisation. The independent role of the DPO as envisaged by the Draft Regulation will also be challenging. Such independence would appear to make it difficult for the DPO to play an integrated role in leading data protection compliance within an organisation. There is a real risk that a DPO could become sidelined by the business and only utilised as a rubber stamp.

- Organisations should take stock of their current processing activities and determine the extent to which the documentation requirements are already met by compliance with their current registration requirements.

- Organisations should review their internal procedures to verify whether the requirements for DPIAs to be undertaken are built into current product development processes.

Section 8 - Individual Rights and Remedies

The rights of individuals have been extended, with some significant changes to existing rights. Under the Draft Regulation, these rights will include a right to "data portability", that is, for the data subject to be given a copy of the data held about him or her in an electronic format, where it is held in a "structured form". Fair processing notices are re-cast as rights of the data subject and the required content set out in detail. The right to object to automated decision making will be replaced by a prohibition on any automated profiling without the consent of the individual. The right to have data erased is re-packaged to include a right "to be forgotten".

The remaining rights, that is, subject access, the right to rectification of inaccurate data, the right to object to processing for direct marketing and unwarranted processing will be largely unchanged. Data subject rights are set out in Chapter III of the Draft Regulation.

All the rights are to be exercisable against data controllers only and not against data processors. However, a supervisory authority will be able to order a data processor to comply with a data subject's request to exercise the rights provided by the Draft Regulation under Article 53(1)(b). This suggests that, if a controller fails to comply with the rights, a processor can be subject to enforcement action.

Data controllers will have to take an holistic view of their obligations to data subjects. They will need to have "transparent and easily accessible" policies covering the rights (Article 11(1)) and ensure that any information provided to data subjects is in clear, plain language, particularly where it is aimed at children. The information to be provided in collection notices is set out in significant detail in Article 14, which includes the periods of retention for the data and information about transfers and disclosures.

The right to rectification in Article 16 will include the right to "completion" of the data by adding a supplemental statement. The three main changes, however, are in the right not to be subject to profiling (Article 20), the right to be forgotten (Article 17) and the right to data portability (Article 18).

Under Article 20, the Draft Regulation bans any measure which produces legal effects or significantly affects an individual which evaluates or analyses a wide range of information including location or preferences or behaviour (profiling) unless: a) it is conducted with the consent of the data subject; b) there is a legal duty to carry out the processing; or c) there is a contract in place with the subject and appropriate safeguard measures to ensure fairness. It is not clear what is meant by the term "significantly affects" but some data protection regulators have stated that they would regard it as covering the delivery of advertising. If the meaning is this wide, it follows that for most businesses any assessment based on automated processing is likely to require consent.

The right to be forgotten in Article 17 comprises two linked rights; the first is the right to erasure or the blocking of data and is relatively straightforward. The second aspect of the right is complex and difficult to follow. It applies where a controller has made data public. If the data subject makes a request, the controller must then take all reasonable steps to inform third parties of the data subject's wish to have the data erased. The right to be forgotten is, however, qualified by the following exceptions: where the processing relates to exercising the right of freedom of expression, the public interest, historical, statistical and scientific research purposes or compliance with a legal obligation to retain the personal data. In relation to freedom of expression, as set out in Article 80, Member States can provide for exemptions from certain provisions in the Draft Regulation (including the right to the forgotten) based on the right of freedom of expression.

The right to data portability is outlined in Article 18 as the right of the data subject to be given a copy of the data held about him or her in an electronic format, where it is held in a "structured form". Such a right is aimed at empowering citizens, making it easier for them to change service providers, e.g., telephone services. Under Article 18 the Commission may specify what is meant be "electronic format".

All of the rights are subject to procedural rules under Article 12 which cover, for example, how controllers must respond to data subjects and impose obligations to give reasons where requests, such as requests to delete data, are refused. In many cases the Commission has reserved the right to make more detailed rules. In some cases these are about procedures, such as standard form fair processing notices or standard form subject access procedures; in other cases these might cover substantive issues, such as the format in which electronic records must be provided to ensure data portability.

Where the rights are not honoured, data subjects have a range of remedies to go to court, seek compensation or to complain to supervisory authorities. Class actions can be brought on behalf of groups of data subjects. A failure to satisfy the rights, even those with more detailed procedural rules, can result in substantial fines from the supervisory authority. The rights may be subject to exemptions but these are not set out in the Draft Regulation. They may be made under EU or Member State law to protect a list of interests including public security, the investigation of criminal offences or the rights and freedoms of others. Data subjects have a right to go to court either in the Member State in which the controller has an establishment or in which the subject is habitually resident, unless the controller is a public authority (Article 75).

Differences from present position

On the face of these provisions, the individual rights do not appear significantly different to those available under the General Directive. For controllers which do conduct profiling activities, and do not make data available to others, there will be relatively little change. For those that do profile and publish data in any way, however, the changes may be significant.

On the changes that will affect all controllers, the following are particularly significant:

- the obligation to have policies and procedures that deal with the exercise of rights;
- the obligations to give reasons for decisions;
- the rights to bring class actions (that is, a group of individuals collectively bringing a claim);
- the right to take action in the State in which the subject has habitual residence even if the controller is in another Member State; and

- the level of detail required in fair processing notices and in response to subject access requests.

Where controllers carry out any form of profiling within the meaning of the new provisions they must have the consent of individuals. Profiling is very widely defined and appears to include actions as simple as analysing data to decide what sort of mailing to send to the individual. It applies where there is a "measure" which "significantly affects" individuals and evaluates some aspect of, or analyses or predicts, their activities. There is no definition of what sort of measure would be regarded as "significantly affecting" someone, so the term may be construed differently by different supervisory authorities.

The right to be forgotten and data portability, at first glance, appear to be new concepts introduced by the Draft Regulation, although a more detailed analysis indicates that such concepts are simply an extension of existing concepts found in the General Directive. The right to be forgotten covers the existing concepts of data destruction and data retention. Similarly, the right to data portability extends the right of subject access by enabling individuals to obtain a copy of their data in electronic form (if it is held in a structured format).

Commentary and Actions

For many data controllers, the area of individual rights is where they have most contact with data subjects and it is these rights which are most often the subject of complaints. The extension of the rights as a way to empower data subjects is regarded by the Commission as one of the key achievements of the Draft Regulation. The Commission has powers to make further rules relating to vexatious use of the subject access right.

As with other provisions in the Draft Regulation, the provisions relating to individual rights are worryingly prescriptive and detailed. Such provisions leave insufficient scope for controllers to find the most appropriate way of dealing with their customers and contacts. Such a prescriptive approach may be driven by the current standards that some data controllers have adopted, for example, by making data subjects who wish to opt out of marketing uses write to a separate address even where the details are being obtained on line.

The right to be forgotten is one of the most controversial provisions in the Draft Regulation. It appears to be targeted at resolving concerns surrounding the retention of personal data online. There are practical challenges for controllers in complying with the right to be forgotten. It is not clear what is meant by making the data public and in many cases controllers will be not be in apposition to notify third parties to whom the data has been disclosed. There are also challenges for controllers even when relying on an exemption under Article 80. For example, where a controller wishes to rely on an exemption made relating to freedom of expression, it would need to consider whether this exemption could be relied upon under the local law of each jurisdiction where the data are processed. The right to data portability is largely unexplained in the Draft Regulation provision.

Regrettably there are no provisions that encourage controllers to work with data subjects, for example, to test and agree the best and most useful kind of notices for a particular industry area.

- Retention periods will become an integral part of the fair processing notice and also the subject access response. If an organisation has not yet adopted retention schedules it would be useful preparation to do so.

- The obligation to have proper statements of policy around the exercise of the rights is unlikely to alter so any organisation which does not yet have a policy on data subjects' rights should put one in place.

- If any form of profiling is carried out, or the publication of information, the organisation should begin to review whether the new provisions (and in particular the requirement to obtain consent to conduct profiling activities) will impact on the business and how they can be complied with.

Section 9 - Exemptions and Exceptions

The Draft Regulation contains a number of exemptions and exceptions which are, largely, similar to the exemptions and exceptions found in the General Directive.

The exemptions and exceptions are set out in several different parts of the Draft Regulation. Some exemptions and exceptions are of general application, and some are limited to particular portions of the Draft Regulation. For example, there are exceptions to the right to be forgotten outlined in Article 17, where the processing relates to exercising the right of freedom of expression, the public interest, historical, statistical and scientific research purposes or compliance with a legal obligation to retain the personal data. In this section the exemptions and exceptions of general application are considered.

The following exemptions and exceptions are significant:

- Article 2: Provides an exemption where the processing is conducted in the context of personal or household activities.
- Article 21: Provides for the EU or Member States to make exemptions relating to, among other things, public security, the prevention, investigation, detection or prosecution of criminal offences, the pubic interest of the EU or a Member State or the protection of the data subjects or the rights and freedoms of individuals.
- Article 80: Provides for Member States to make exemptions relating to the safeguarding of freedom of expression.
- Articles 25, 28 and 35: Provide for SMEs with fewer than 250 employees to be exempt from requirements contained in these Articles.

Article 2 provides an exemption from the general restrictions on processing personal data in circumstances where processing is undertaken by an individual without any "gainful interest", in the course of personal or household activities. This is largely unchanged from the exemption contained in the General Directive. Any processing for such purposes is exempt from the scope of the Draft Regulation.

Article 21(1) provides that the EU and/or Member States may pass legislation to implement exemptions to the restrictions on processing personal data contained in the Draft Regulation. Exemptions may be made to safeguard, amongst other things:

- public security;
- the prevention, detection, investigation and prosecution of criminal offences;
- public interests of the EU or Member States, including financial and economic interests in particular;
- the regulation and enforcement of ethical standards in regulated professions; or
- data subjects or the rights and freedoms of individuals.

Any exemption made in relation to the above must constitute a necessary and proportionate measure in a democratic society. Therefore, while Member States have considerable scope to provide for exemptions, the exemptions will need to be proportionate to the interests to be safeguarded. As individual Member States will pass legislation to provide for exemptions, this means that exemptions will be applicable to particular Member States and will not be harmonised across Member States.

Article 80 of the Draft Regulation permits Member States to implement exemptions or derogations for the purpose of freedom of expression where the processing is carried out solely for journalistic, artistic or literary purposes.

SMEs will benefit from a number of exemptions. Under Article 28(4), the obligation to keep detailed documentation of processing activities does not apply to organisations which employ fewer than 250 people and the processing is auxiliary to its main activity. Similarly the requirement to appoint a DPO under Article 35, only applies to data controllers with more than 250 employees. Finally under Article 25(2) an organisation with fewer than 250 employees is exempt from the requirement to appoint a representative in the EU if it is not established in the EU but processes data related to either: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour.

Differences from present position

The Draft Regulation includes provisions which allow for exemptions to be made by Member States which restrict the scope of the Draft Regulation in certain circumstances. This will allow the local laws of Member States and some cultural differences to be taken into account. There are no significant differences between the subject matter of the exemptions that can be made by Member States under the Draft Regulation and those under the General Directive. They relate to broadly the same categories of interests.

The provision in the Draft Regulation for exemptions to be made to safeguard the freedom of expression will ensure a balance is achieved between the protection of personal data and freedom of expressions.

The inclusion of several exemptions for SMEs in the Draft Regulation is different from the present position under the General Directive, where all data controllers have essentially the same legal obligations, regardless of the size of their business or organisation. Given the increase in the number of administrative measures to be implemented, these provisions will be welcome by SMEs.

Commentary and Actions

Whereas the General Directive exempts the processing of personal data in the context of personal or household activity, the Draft Regulation exempts such processing only insofar as the person performing the processing has "no gainful interest" in that processing. It is not entirely clear what this adds. The UK ICO has requested clarification that, for example, "personal commercial activity – such as selling one's personal possessions" should fall within this exemption, notwithstanding the fact that there is a clear "gainful interest" for the seller.

It appears that further consideration is required in order to ensure that the exemptions and exceptions set out in the Draft Regulation will work in practice. For example, the EDPS has commented that the provision allowing for a public interest exemption in Article 21 (relating to the exemptions from the provisions of the Draft Regulation) is too broad and ill-defined, and that this exemption should be limited to clearly identified and limited circumstances, including criminal offences or economic and financial interests.

- Organisations should consider whether they fall within the definition of an SME, that is they have fewer than 250 employees and any processing of personal data is auxiliary to their main activity. This will allow the organisation to take advantage of the exemptions for such organisations in the Draft Regulation.

Note

This Briefing Paper has been produced by the Hunton & Williams Privacy and Information Law Team for use by clients. If you would like to receive an electronic copy, please contact Bridget Treacy (btreacy@hunton.com), Wim Nauwelaerts (wnauwelaerts@hunton.com) or Rosemary Jay (rjay@hunton.com).

This Briefing Paper should be used as general guidance only and should not be relied upon as advice. If you require advice please speak to your usual contact at Hunton & Williams to discuss your needs. The material is intended to help your organisation start to prepare for the important changes that will occur in the field of data protection compliance. You are welcome to use it provided you credit Hunton & Williams using the copyright wording at the end and use is limited to within your organisation. If you know of anyone else who would find it useful, please feel free to pass our contact details to them and we will be happy to supply an electronic copy.

HUNTON& WILLIAMS

Executive Briefing Paper - Update

Proposed General Data Protection Regulation

Update 1
January 2013
Draft LIBE Report to the European Parliament

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Hunton & Williams
30 St Mary Axe
London
EC3A 8EP
United Kingdom

Introduction

On 25 January 2012, the European Commission released its widely anticipated data protection legislative framework proposal, intended to replace Directive 95/46/EC. The Commission's proposal consists of two instruments: a general data protection regulation (the "Draft Regulation") and a directive on processing personal data in relation to police and criminal justice matters.

On January 10, 2013, the Rapporteur to the European Parliament, Jan Albrecht, presented his report on the Draft Regulation to the Committee on Civil Liberties, Justice and Home Affairs ("LIBE committee"). The report is detailed and addresses many of the issues raised in the past 12 months. The results will not be universally welcomed. The proposals would increase the burdens on data controllers in several areas, however, elements of the report, such as the clarification of the "right to be forgotten", are likely to be welcomed.

The Rapporteur's proposed amendments would have an impact on the balance of power between the Commission and the Parliament. Many of the proposed amendments would reduce the Commission's powers, in large part transferring them to the European Data Protection Board (the intended successor to the current Article 29 Working Party). Further, some Commission decisions (e.g., adequacy findings) would require a delegated act under the proposed amendments, thereby giving the Parliament the opportunity to reject the decision.

This report is not the end of the story. It has yet to be debated by the Parliament which may well make its own changes. Further, some of the drafting of the report is patchy and unclear and requires further clarification and amendment in order to make the proposed changes clear and coherent. Parliament will be tabling amendments up until the LIBE committee is due to reconvene and discuss the amendments, currently scheduled for February 27, 2013. Once the views of the Parliament have crystallised it will then be for the Council and the Commission to consider the recommendations. The process has a long way to go still; businesses should therefore not be panicked by these proposed changes, but remain engaged in and provide feedback on the discussion.

In this Update we have flagged those proposals which would have a significant impact if they were to be adopted. The Update follows the pattern of our Executive Briefing paper and, like that paper, can be used as a basis for internal briefings.

This Update is divided into the same nine sections as the Executive Briefing paper covering:

1. Definitions
2. Scope
3. Data quality principles
4. Overseas transfers
5. Security
6. Supervisory authorities
7. Internal controls
8. Individual rights
9. Exemptions

Section 1 - Definitions

The report proposes 4 new definitions: "producer", "profiling, "transfer" and "pseudonym," in order to accommodate new provisions.

"Producer" would be defined as "*a natural or legal person, public authority, agency or any other body which creates automated data processing or filing systems designed for the processing of personal data by data controllers and data processors*". A note at Amendment 98 refers to "producers" as "producers of automated data processing systems (i.e. hard- and software)." The inclusion of this additional definition would assist in protecting personal data throughout the entire data life cycle. Producers would be subject to obligations of data protection by design and by default, as well as data security. However, as producers are not covered by the sanctions provisions, currently there would be no enforcement mechanism to ensure compliance with these requirements.

"Pseudonym" would be defined as "*a unique identifier which is specific to one given context and which does not permit the direct identification of a natural person, but allows the singling out of a data subject*". It is unclear exactly what this definition means, and whether it would reflect the concept of "identifiability". The inclusion of this new definition accommodates further clauses on the processing of pseudonymised data and provisions on the pseudonymous use of services, including being able to make subject access requests pseudonymously. For example, if an individual had signed up to use an online service using a selected username only, and without having to supply their real name, they would also be able to make subject access requests using their username without having to supply their real name. This can be seen as reflecting certain current local law requirements, e.g., in Germany, where data subjects have a right to use online services pseudonymously.

A "transfer" of personal data would be defined as "*any communication of personal data, actively made available to a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data*." An additional definition of a "transfer" of personal data, as opposed to the commonly used yet undefined term of "disclosure", is justified at Amendment 86 as being required in order to distinguish it from making data publicly available. The new definition is introduced in order to tighten up the provisions on the right to be forgotten and make them more practical. Accordingly, data controllers would only be required to inform third parties of erasure requests where the personal data had been transferred to them specifically, knowingly or intentionally, as opposed to where personal data had been published widely and made available to unspecified third parties. It is not clear how the new definition would impact on international data transfers.

"Profiling" would be defined as "*any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour*". In addition to the introduction of a specific definition of "profiling", requirements are proposed for notice to individuals and informed consent for profiling activities. Under the Commission's draft, profiling is expressed as a right (the right not to be subject to measures based on profiling), although in effect it operates as a prohibition, as profiling is prohibited unless specific circumstances apply (Art. 20(2)). The proposed amendments clarify that profiling is subject to a general ban.

Additionally, a number of amendments to existing definitions are proposed:

- "Data subject" would be amended to introduce the concept of the ability to "single out" a natural person. It is unclear how this notion differs from the current concept of "identifiability".
- "The data subject's consent" would be amended to clarify that consent must be given for specific purposes.
- "Personal data breach" would be amended to clarify that a data breach can occur without a security breach, e.g., by accidental loss or disclosure.
- The special categories of personal data (i.e., sensitive personal data) would be extended to include philosophical beliefs, sexual orientation or gender identity, and trade-union activities.

Section 2 - Scope of the Draft Regulation

The extra-territorial scope of the Draft Regulation would be extended to include data controllers outside the EU who aim services at EU citizens, irrespective of whether the offered goods and services are paid for or free or charge, and which monitor EU citizens in any way (i.e., not just those which monitor the behaviour of data subjects).

Recitals 23 and 24 would be amended to clarify that the Draft Regulation would not apply to anonymous data, being data which "*cannot be related, directly or indirectly, alone or in combination with associated data, to a natural person or where establishing such a relation would require a disproportionate amount of time, expense, and effort, taking into account the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed*". It is unclear to whom the disproportionate effort requirement would apply (i.e., the data controller or third parties). In the UK, existing case law on the release of pseudonymised or barnadised data (for statistical purposes) makes clear that the test of identifiability of individuals from the data applies to whether members of the public would be able to identify individuals from the data (i.e., the "motivated intruder" test), not whether the data could be re-identified by the data controller from other data in its possession.

Further, where a data controller processes pseudonymous data which do not single out or identify a natural person, the data controller would not be required to obtain additional information in order to identify the data subject so as to comply with the requirements of the Draft Regulation.

The exemption for domestic processing would be extended to cover personal commercial activity, such as selling possessions on eBay.

Section 3 - Data Quality Principles

The "legitimate interest" legal basis for the processing of personal data would be drastically restricted for use in "exceptional circumstances" only. Currently many data controllers, particularly in jurisdictions such as the UK, rely on the legitimate interest ground for much of their processing activities. The amendments indicated in the draft report would significantly tighten the scope of the ground, including new requirements for a data controller to provide notice to data subjects that it is relying on the ground, and to publish the reasons for believing that its legitimate interests would override the data subjects' fundamental rights and freedoms. The amendments set out certain circumstances which would constitute a legitimate interest, including enforcement of legal claims, debt collection, civil damages or remedies. The amendments also specify circumstances where the interests and fundamental rights and freedoms of the data subject would, as a rule, override the interests of data controllers, including where the data subject does not expect further processing; the processing causes a serious risk of damage to the data subject; the processing relates to sensitive personal data, location data or biometric data; personal data are processed in the context of profiling; and where the data subject is a child.

Amendments to Recitals 33 and 34 clarify that consent could not be validly obtained: (i) through the use of default options which would require a positive action to object, as opposed to a positive action to consent (e.g., unchecking a pre-checked box); (ii) where the controller or processor were in a dominant market position with respect to the products or services offered to the data subject; or (iii) in relation to unilateral and non-essential changes in terms of use to services. Data subjects would be able to provide consent without having to identify themselves, e.g., in the pseudonymised use of services. The execution of a service contract could not be made conditional upon the data subject providing consent to the processing of their personal data for purposes which are not necessary for the provision of the service.

Section 4 - Overseas Transfers

The report rejects the inclusion of "processing sectors", in addition to countries and territories, as eligible for being deemed adequate by the Commission. The justification provided in the report is that recognising processing sectors as adequate would increase "legal uncertainty and undermine the Union's goal of a harmonised and coherent data protection framework". Further, adequacy findings would be made by the adoption of a delegated act, empowering the Parliament to reject Commission adequacy proposals. Existing adequacy findings (including the U.S.-EU Safe Harbor framework) would only remain in force for a period of two years after the implementation of the Draft Regulation, which would provide a short timeframe for the Commission to review and renew all of the existing adequacy findings, making additional adequacy findings unlikely during the initial period. The deadline for expiry would also create confusion as to the wisdom of self-certifying to Safe Harbor in the interim period between now and the implementation of the Draft Regulation. Similarly, the Commission decisions approving the adequacy of Model Clauses would also only remain in force for two years after the Draft Regulation takes effect, instead of remaining in force until replaced or repealed by the European Commission.

A significant extension of control is proposed in relation to overseas transfers where every transfer based on a derogation, such as data subject consent, would require prior submission to the supervisory authority. This would greatly increase the burden of relying on derogations for transfers.

The report also inserts new provisions addressing data transfer requests from courts and authorities in third countries which would impose the requirement to obtain prior authorisation from the national supervisory authorities in certain cases.

Section 5 - Security and Breach Notification

The definition of "personal data breach" would be amended to clarify that a data breach can occur without a security breach, e.g., by accidental loss or disclosure.

Where data controllers are required to notify breaches to data subjects, they would further be required to inform data subjects of their rights, including the possibility of redress.

The timeframe for reporting data breaches to the supervisory authority would be extended from 24 hours to 72 hours; a change which is likely to be welcomed. Less likely to be welcomed, the supervisory authority would maintain a public register of notified breaches. The details which would be published in the register are not specified, but such public naming and shaming is not likely to be met with approval from data controllers.

Section 6 - Powers of Supervisory Authorities and the Commission

Each supervisory authority would oversee the processing operations which take place on the territory of its state and processing operations outside its own territory where the personal data of its residents are being processed. Therefore an authority could supervise processing outside its jurisdiction and some data controllers and data processors would be subject to the supervision of more than one authority. However, all supervisory authorities would be required to cooperate with each other and the only authority which could take action against a controller or a processor would be the one for the jurisdiction in which the entity had an establishment. This would give rise to practical difficulties in taking enforcement actions against controllers which have no establishment in the EU but process personal data about EU residents. It is possible that actions would be taken against the representative.

The concept of a "lead authority" would therefore undergo a dramatic change. If a controller or processor were established in several countries the lead authority would remain the authority for the country in which the

controller or processor has a main establishment. However, its role would be reduced to that of a post-box and coordinator. In other words, all contact with the controller would be routed through the lead supervisory authority.

Although the new provisions would mean the end of the supervisory role of the lead authority there would be no corresponding diminution of the powers of authorities to impose monetary penalties therefore a company which operated from a number of countries could be subject to the maximum penalty in each country.

The role of the Commission in dealing with enforcement would be very much reduced. It could only express a strong opinion where it disagreed with a proposed enforcement action. If the Commission wished to challenge an action it would have to do so before the Court of Justice of the European Union.

The consistency mechanism would remain in place but its remit would change as there would be far fewer cases in which it would be required to adjudicate between authorities. The main example would be where an entity operates from one location in the EU but its actions affect the residents of many EU countries.

A new provision would allow the European Data Protection Board to determine which authority should be the lead authority if the designation were unclear or disputed. This seems useful, although it would be better if it were linked to the appointment of the representative. It is possible that a company could appoint a representative in one country but the Board appoint a lead authority in another.

There would also be some bolstering of the position of independence of the supervisory authorities.

Section 7 - Prior Notice to Supervisory Authorities and Internal Controls

The Commission draft of January 2012 replaced the system of notification to supervisory authorities with a system of internal record keeping by controllers, processors and representatives. The Rapporteur's proposals would replace the internal records, at least for data controllers, with personalised notifications to data subjects. These would be a form of greatly extended privacy notice. They would include all the information required by the Commission, plus information about profiling and how to object to profiling, information on rights to object to the processing of personal data and reasons for believing that the controller is entitled to rely on legitimate interest as a basis for processing. The amendments appear to have relieved data processors of the obligations to maintain these records, however, this may be a mistake in the drafting.

Data Protection Impact Assessments ("DPIAs") would become routine for almost all new processing as the circumstances in which they would be required are greatly extended. These would be required for all uses of sensitive personal data, all processing of personal data of children and any surveillance. DPIAs would also be required in cases where personal data are made available to a large number of persons, which would presumably catch all professional firm websites. DPIAs are tightened in other ways; for example, there must always be consultation with data subjects, irrespective of the commercial sensitivity of the processing.

Changes are proposed to the provisions which require prior submission of new processing operations to the supervisory authority. Where DPIAs have been carried out in respect of such new operations, they may be considered by the data controller's data protection officer ("DPO").

The threshold for the appointment of a DPO would be altered so that it is related to the number of data subjects about whom data are processed. A DPO would be required if the controller or processor undertakes profiling or core activities involving sensitive personal data. Further, all controllers would be required to notify the supervisory authority if they did not appoint a DPO and to justify that decision.

Section 8 - Individual Rights and Remedies

There are some useful clarifications to the rights of individuals but also some ill-conceived and difficult proposals. The provisions on data collection and privacy notices have become difficult to understand. The notice to data subjects when data are collected would become the detailed statement described in the previous section. It is no longer clear what the "ordinary" notice to data subjects would contain. The new notice would also be delivered in "icons" to be specified by the Commission after consultation with the Board. The data subject could still obtain detailed information on request. There would be a significant overlap between the information to be provided on subject access, and that to be provided in the collection notice.

Where data have been rectified, individuals would be given rights to know who has been notified of rectification; an amendment which would be helpful and should not be onerous.

A subject access request would also elicit information as to whether the data controller has undertaken profiling or made decisions based on profiling, the consequence of any measures based on profiling, information about the logic in any automated decision making, as well as any disclosures to public authorities. The right to data portability would be absorbed into the right of subject access so that where data is supplied in electronic form, it would have to be supplied in a portable format which is "structured" and "commonly used".

The "right to be forgotten" would be much simplified and improved. A distinction would be drawn between cases where the controller has made a positive disclosure and those where the data have been made public without justification.

The right to object to data processing would also be simplified and the provision dealing with profiling made clearer, although more onerous for controllers. Sensitive personal data could not be used in profiling, nor could profiling be used to identify children. Profiling would also be prohibited if the effect would be discriminatory on the basis of the sensitive categories of personal data, e.g., race, religion.

Section 9 - Exemptions and Exceptions

Member States could still provide for exemptions from the requirements of the Regulation, but the grounds would be tightened. For example, it would no longer be possible to provide for exemption for the purpose of official monitoring for public security or policing or the protection of economic interests. In addition, any exemption would need to be proportionate.

The exemption for freedom of expression would specifically reference that right (rather than referring to journalism) and the rights in the EU Charter of Fundamental Rights.

Some exemptions for SMEs would be removed and those that remain (e.g., the requirement to appoint a DPO and to appoint an EU representative) would apply to organisations that process personal data on fewer than 500 individuals, rather than being assessed by reference to the number of employees.

There would also be proposed changes to the exemption for medical research, which would limit those cases in which research could be conducted without consent.

Note

This Briefing Paper has been produced by the Hunton & Williams Privacy and Information Law Team for use by clients. If you would like to receive an electronic copy, please contact Bridget Treacy (btreacy@hunton.com), Wim Nauwelaerts (wnauwelaerts@hunton.com) or Rosemary Jay (rjay@hunton.com).

This Briefing Paper should be used as general guidance only and should not be relied upon as advice. If you require advice please speak to your usual contact at Hunton & Williams to discuss your needs. The material is intended to help your organisation start to prepare for the important changes that will occur in the field of data protection compliance. You are welcome to use it provided you credit Hunton & Williams using the copyright wording at the end and use is limited to within your organisation. If you know of anyone else who would find it useful, please feel free to pass our contact details to them and we will be happy to supply an electronic copy.

HUNTON& WILLIAMS

Executive Briefing Paper - Update

Proposed General Data Protection Regulation

Update 2
June 2013
Draft Compromise Text Proposed by the Irish Presidency to the Council of the European Union

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Hunton & Williams
30 St Mary Axe
London
EC3A 8EP
United Kingdom

Introduction

On May 31, 2013, the Justice and Home Affairs Council of the European Union released a draft compromise text on the European Commission's proposed General Data Protection Regulation (the "Regulation"). This compromise text narrows the scope of the Regulation and seeks to move from a detailed, prescriptive approach towards a risk-based framework.

The Council of the European Union is composed of the ministers of the Member States and, together with the European Parliament, acts in a legislative capacity, usually in response to proposals from the European Commission. The Presidency of the Council rotates among Member States every six months, with each Presidency developing initiatives and setting the Council's agenda during the six month term. The current Presidency is held by Ireland until July 1 with Lithuania holding the Presidency for the second half of 2013. The Irish Presidency has made the Regulation a particular focus of its term.

The European Commission published the draft Regulation in January 2012. Over the last 18 months, the Regulation has been the subject of intense negotiations, re-drafts and media speculation in Brussels and across the EU. In January 2013, the appointed rapporteur of the lead Parliamentary committee, Jan Philipp Albrecht, issued the Civil Liberties, Justice and Home Affairs ("LIBE") Committee's draft report on the Regulation, proposing a number of significant amendments (*see* Update 1 to the Executive Briefing). A further four committees of the European Parliament also released opinions proposing amendments. In total, over 3,000 amendments to the Regulation have been proposed, resulting in the LIBE Committee postponing its orientation vote, which had originally been scheduled for March and delayed until May 29, 2013.

The LIBE Committee is currently considering the tabled amendments and preparing a compromise text for the European Parliament to vote on. The next step will then be for the European Parliament and the Council of the European Union to negotiate the finalised text. Given the forthcoming summer recess, these negotiations are not expected to take place before September 2013.

In anticipation of the negotiations between the European Parliament and the Council of the European Union, the Irish Presidency of the Council has prepared compromise text for the Council to consider. The Presidency's proposed amendments are limited to Chapters I – IV of the Regulation only, and so do not offer amendments on issues addressed in later chapters, including international data transfers, powers of the supervisory authorities, or sanctions.

The draft compromise text tempers many of the European Commission's original proposals that were the subject of some of the most vociferous debate. In particular, it narrows the scope of the Regulation and seeks to move from a detailed, prescriptive approach towards a risk-based framework. The Presidency also emphasises that no single part of the Regulation can be finally agreed until the text of the whole Regulation is agreed.

In this Update we have flagged those proposals which would have a significant impact if they were to be adopted. The Update follows the structure of our Executive Briefing paper and, like that paper, can be used as a basis for internal briefings.

This Update is divided into the following sections:

1. Choice of legislative instrument
2. Definitions
3. Scope
4. Risk-based approach and pseudonymisation
5. Data quality principles
6. Security and breach notification
7. The role of supervisory authorities and the Commission
8. Internal controls and codes of conduct
9. Individual rights

Section 1 - Choice of Legislative Instrument

The Presidency notes that eight Member States (Belgium, the Czech Republic, Denmark, Estonia, Hungary, Sweden, Slovenia, and the UK) still do not support the Commission's choice of legislative instrument as a regulation, and would prefer that the current EU Data Protection Directive (Directive 95/46/EC) is repealed and replaced by another directive. The Presidency's proposed amendments leave flexibility for the proposed Regulation to be transformed into a directive in the future. The Presidency has therefore not ruled out the possibility of a change of instrument.

While the possibility of recasting the Regulation as a directive remains, the Presidency's proposed amendments emphasise that differing levels of data protection within the European Union must not impede the free flow of personal data within the Union (Recital 11).

Section 2 - Definitions

The definition of "data controller" is amended such that the controller determines the means and purposes of the processing, but does not also have to determine the conditions of processing (Article 4(5)).

The definition of sensitive personal data is amended to exclude data concerning criminal convictions or related security measures (Article 9(1)). This preserves the current position under Directive 95/46/EC, which is reflected in many national implementing laws (although not all, e.g., the UK Data Protection Act 1998).

The amendments introduce an additional category of data which are neither deleted nor actively processed, but marked for restricted processing (Article 4(3a)).

An additional category of "pseudonymised" data is proposed at Article 4(2a), being "personal data processed in such a way that the data cannot be attributed to a specific data subject without the use of additional information, as long as such information is kept separately and subject to technical and organisational measures to ensure non-attribution". The definition characterises pseudonymised data as a sub-category of personal data, rather than a third type of data along with anonymous data, or a sub-category of anonymous data. This may assist in arguments that encrypted data can be considered as pseudonymised data, which has repeatedly been classed as personal data by Commissioner Reding and the European Data Protection Supervisor, Peter Hustinx. This new definition will also likely greatly assist UK data controllers, as under the Data Protection Act 1998, the concept of personal data extends not only to data which could identify affected data subjects, but also the combination of those data and other data in the possession of, or likely to come into the possession of, the data controller. This new concept of keeping additional information separately, including within organisations (e.g., using Chinese walls), in conjunction with the introduction of the pseudonymisation of data as a lawful processing ground, will significantly ease controllers' obligations in relation to processing pseudonymised data.

A definition of "profiling" is included at Article 4(12a) as "any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to a natural person, in particular the analysis and prediction of aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements".

The definition of "enterprise" (Article 4(15)) is amended to include natural persons engaged in an economic activity (e.g., one-person tech start-ups and paid-for bloggers, etc.).

The definition of "child" as someone below 18 years of age is deleted (Recital 29 and Article 4(18)).

Section 3 - Scope of the Regulation

The Presidency proposes parallel amendment of Regulation 45/2001 (on the protection of individuals with regard to the processing of personal data by the Community) to bring the processing activities of European Union bodies within scope of the Regulation (Recital 14a, Article 2(b)). Latitude is, however, granted to public bodies in a number of amendments, including clarification of public access to official documents for public interest purposes, and recognition of the ability of public bodies to respond to information requests under freedom of information statutes.

The proposed amendments further clarify the extraterritorial application of the Regulation to data controllers located outside of the EU. Recital 20 explains that mere accessibility of a controller's website from within the EU would not constitute "the offering of goods or services" under Article 3(2)(a) and that whether the controller appears to "envisage" doing businesses with EU data subjects is a determining factor. Whether a controller "envisages" doing business with EU data subjects can be ascertained from the functionality of a controller's website, including local language and currency. The amendments also delete Recital 64 of the Commission's proposals, which included within scope of the Regulation data controllers "occasionally" offering goods or services to EU data subjects.

The Presidency's amendments further clarify the extraterritorial application of the Regulation to data controllers located outside of the EU in relation to those which monitor the behavior of EU data subjects (Article 3(2)(b)). The monitored behaviour must take place within the EU, and so the Regulation would not apply to monitoring the behaviour of data subjects habitually resident in the EU, but temporarily based outside of the EU.

Regulation 23 of the Presidency's proposals emphasises that the principles of data protection do not apply to the processing of anonymous data or personal data relating to the deceased. Whether information is considered as "anonymous" depends in part on the costs and the amount of time required to identify the data subjects to whom the data relate. This clarification will no doubt be welcomed by data controllers, given the practical and technical difficulties of achieving complete and permanent anonymisation.

The proposed amendments clarify that, under the household exemption, the Regulation does not apply to social networking and online activities by individuals, provided that they are undertaken as a household activity (i.e., not sponsored or paid-for bloggers, etc.).

Section 4 – Risk-Based Approach and Pseudonymisation

Overall, the Presidency's proposed compromise text can be seen as more business-focused and as offering a more pragmatic approach. Specifically, the Presidency proposes an additional recital (Recital 3a), clarifying the right to data protection as a qualified right, highlighting the principle of proportionality and importance of other competing fundamental rights, including the freedom to conduct a business.

The principles of proportionality and context are consistent themes throughout the Presidency's proposed amendments. In particular, the compatibility of further processing purposes is dependent on a number of factors, including the context of collection, and: (i) any link between the original purposes and intended further purposes; (ii) the reasonable expectations of further use anticipated by the data subject; (iii) the nature of the personal data; (iv) the consequences of the further intended processing for data subjects; and, (v) appropriate safeguards.

Proportionality and a risk-based approach is also particularly reflected in the Presidency's revision of the documentation requirements proposed by the Commission. Where Recital 60 had required that data controllers should be "obliged to demonstrate the compliance of each processing operation with this Regulation," the Presidency suggests that controllers demonstrate their compliance in more general terms, keeping records and conducting data protection impact assessments ("DPIAs") depending on the nature, scope, context and purposes of specific processing activities and the associated risks to the rights and

freedoms of data subjects. These risks are to be viewed against a backdrop of physical, material or moral damage to data subjects, including discrimination, identify theft, financial loss, and reputational damage.

Processing pseudonymised data is a key tool in the risk-based framework. Under new Article 10(2), where a data controller is "not in a position to identify the data subject" critical substantive requirements under the Regulation do not apply, namely Articles 15 (right of access), 16 (right of rectification), 17 (right to be forgotten and to erasure), 17a (right to restriction on processing), 17b (notification obligations regarding rectification, erasure or restriction), and 18 (right to data portability). These broad exemptions would also greatly assist controllers processing pseudonymised data. Affected data subjects are, however, permitted to provide additional information enabling their identification such that these broad exemptions at Article 10(2) do not apply.

Section 5 - Data Quality Principles

The principle of data minimisation is excluded as an explicit obligation. References to data minimisation are deleted, including at Recital 30 and Articles 5(c) and 23(2). This will likely be welcomed by data controllers, particularly those in sectors which are heavily dependent on big data analysis, such as insurance, finance, advertising, retail, and technology.

The application of the principles of data protection by design and default are limited, dependent on the available technology and the risks posed to data subjects (Article 23(1)). Processing pseudonymised data is explicitly called out as a data protection by design and default measure.

The legitimate interests basis for lawful processing (Article 7(f) of Directive 95/46/EC) is explicitly extended to include: (i) fraud prevention; (ii) anonymising or pseudonymising personal data; and, (iii) direct marketing purposes. The first extension will likely be particularly welcomed by data controllers operating in the financial and retail sectors. The second extension reflects calls widely made, including by Commission Vice-President Viviane Reding, to incentivise the processing of anonymous and pseudonymous data in place of personal data. The third extension will likely cause the most surprise and may not be unanimously welcomed, although it could be said to reflect current practice in more permissive jurisdictions, such as the UK.

The establishment, exercise or defence of legal claims is introduced as a further specific ground for the lawful processing of sensitive personal data. This additional lawful processing ground could, in particular, assist data controllers processing personal data in the context of discovery requests.

The criterion for valid consent is amended from "explicit" to "unambiguous", except in the case of processing special categories of data (i.e., sensitive personal data) (Recital 25 and Article 9(2)). This reverts to the current position under Directive 95/46/EC and is a concession to the practical difficulty of obtaining explicit consent in all cases.

The criteria for valid consent are further relaxed by the ability to obtain consent in writing, orally or in an electronic manner. Where technically feasible and effective, valid consent can be given using browser settings and other technical solutions. Further, the requirement that the controller bears the burden of proof that valid consent was obtained is reduced to a requirement that the controller be able to "demonstrate" that consent was obtained (Recital 32 and Article 7(1)). The need for "informed" consent is also relaxed from the requirement to provide the full information requirements laid out in Article 14 to the minimal requirements that the data subject is "at least" made aware of: (i) the identity of the data controller; and (ii) the purpose(s) of the processing of their personal data (Recitals 33 and 48).

The Commission's proposal required separate and distinguishable written consents for processing for different purposes (Article 7(2)). This obligation is alleviated by the requirement to present the request for consent for separate matters in a distinguishable manner, rather than the given consents themselves being distinguishable. Data controllers would therefore not be prevented from obtaining written consent to multiple processing activities, provided clear and distinguishable notice of each different processing activity was provided.

Under the Commission's proposals, valid consent cannot be given where a significant imbalance exists between the data subject and the data controller, e.g., in the employment context. This is tempered in the Presidency's draft by the shift from a default assumption that valid consent cannot be obtained to an assessment in each specific situation (Recital 34).

Appointment of a sub-processor by a data processor no longer requires, by default, the controller's prior permission (Article 26(2(d)). Processors who act beyond the controller's instructions are no longer automatically considered to be a joint controller (Article 26). Certain obligations would no longer apply to data processors, including conducting DPIAs (Article 33).

The provisions concerning data retention in the Commission's proposals are significantly relaxed in the Irish Presidency's proposed text. In particular, controllers are not obliged to provide notice of specific retention periods (Articles 14, 15 and 28).

Section 6 - Security and Breach Notification

A new principle of data security is introduced (Article 5(1)(ee)). The principle of data security has limited application, dependent on the available technology and the risks posed to data subjects (Article 30(1)). Processing pseudonymised data is explicitly indicated as a data security measure.

As expected, the timeframe for reporting personal data breaches is extended from 24 hours to 72 (Recital 67 and Article 31). Further, only significant breaches which may result in "severe material or moral harm" must be notified to the competent supervisory authority (Recital 67 and Article 31). This amendment greatly ameliorates the Commission's proposals, which required notification of all data breaches and did not specify any threshold requirements. Similarly, the Presidency proposes that only severe breaches must be notified to affected data subjects, and that notification to both the supervisory authority and to data subjects is not required where technological measures applied to the personal data mean they are unintelligible to third parties, or where the breach affects pseudonymised data which would also be unintelligible to third parties (Recital 68a and Articles 31(1a) and 32(3)(a)). Further, notification to data subjects is not required where the controller takes subsequent steps to protect affected data subjects (Article 32(3)(b)). In addition, where it would involve disproportionate effort to notify data subjects individually, the controller may instead make a public communication (Article 32(2)(c)).

Section 7 – The Role of Supervisory Authorities and the Commission

The role of supervisory authorities in the context of DPIAs is reduced from one of prior checking and authorisation to providing advice (Recital 74). In relation to international data transfers, controllers would no longer be required to obtain prior authorisation for transfers based on standard contractual clauses (Article 34(1)).

A particular criticism of the Commission's proposal is the number of instances throughout the Regulation where the Commission reserves the power to legislate further, in the form of delegated and implemented acts. This would cast uncertainty over the Regulation as it could be further amended and changed at any time, leaving controllers and processors uncertain of their obligations and unable to make long-term business decisions. The Presidency's proposed text deletes all implemented acts and all but one power to adopt delegated acts (Article 39a) in Chapters 1 – IV.

Section 8 – Internal Controls and Codes of Conduct

DPIAs would be the sole responsibility of data controllers, and not processors (Article 33(1)). The list of processing operations requiring DPIAs at Article 33(2) is made an exhaustive, not indicative, list. Under Article 33(2)(a), DPIAs are required only for profiling activities which would "severely" affect data subjects. In conducting a DPIA, data controllers would no longer be required to seek the views of data subjects or their representatives (Article 33).

Under Article 34, supervisory authorities would no longer have the power to prohibit processing activities submitted for prior consultation following the conduct of a DPIA. The supervisory authority would be required to provide advice to data controllers within six weeks of receipt of a DPIA (extended by a further month in the case of complex processing activities) (Article 34(3)).

The appointment of a data protection officer (DPO) is re-cast as optional, unless stipulated by national law (e.g., as is currently the case in Germany for many organisations). The minimum tenure of two years proposed by the Commission is deleted. The tasks of the DPO are reduced and no longer include monitoring the implementation and application of the Regulation, the documentation requirements, breach notification and the conduct of DPIAs.

Codes of conduct and certification play a more prominent role in the Presidency's proposed draft, in particular in relation to demonstrating privacy by design and default, as a kite mark for processors sufficiently guaranteeing processing in accordance with the requirements of the Regulation, and in relation to data security measures.

Section 9 - Individual Rights and Remedies

The information that must be provided to data subjects is greatly reduced from the lengthy list originally set out in Articles 14(1)(a) to (1)(h) to two key requirements: (i) the identity of the data controller; and (ii) the purpose(s) of the processing of their personal data (Article 14(1)(a) & (b)). Further specific notice, including of intended international data transfers and profiling activities, must be provided where required to ensure fair and transparent processing in the specific circumstances. The data controller is also not required to provide notice where the data originate from publicly available sources (Article 14a(4)(c)). This will greatly reduce the burdens on those controllers which process large amounts of publicly available data, including advertisers and recruiters who "scrape" publicly available personal data from social media profiles.

The prohibition on profiling applies to decisions based on profiling, rather than profiling measures, more closely reflecting the current restrictions on automated decisions under Article 15 of Directive 95/46/EC. This significantly narrows the scope of the profiling provisions and will no doubt be welcomed by data controllers. Further, the restriction only applies where the decision would produce legal affects severely affecting the data subject.

Processing for profiling purposes is expressly permitted for the purposes of fraud monitoring and prevention and to ensure the security and reliability of services provided by controllers. The latter provision may be particularly pertinent in the context of cyber security. Profiling can be based solely on sensitive categories of data, provided the data subject's explicit consent is obtained and suitable measures to safeguard the data subject's legitimate interests have been implemented (Article 20(3)).

In the Commission's draft, the right to be forgotten and to erasure is not cleanly separated as two obligations. In the Presidency's proposal, the separate rights of erasure and abstention from further processing are separated out into two separate articles: 17a and 17b. Article 17b provides that personal data which are contested, objected to, or no longer required by the controller (but are required by the data subject), are not deleted, but are restricted from further processing.

In the Presidency's re-draft, it is made clear that the data controller is only required to notify third-party recipients of the data of the data subject's erasure request where that request meets the erasure criteria and

so would be a successful request (i.e., where the controller would be required to erase the data). If the controller is not required to erase the data, it is also not required to notify third parties of the data subject's erasure request. The requirement to notify third parties is also further limited from "all reasonable steps" to "reasonable steps" in the circumstances, taking into account available technology and the cost of implementation (Article 17(2a)). This would likely greatly reduce the burden of processing erasure requests for intermediaries such as search engines and social networks.

The right to object is limited to personal data processed on the grounds of the legitimate interests basis and does not cover personal data processed on the grounds of necessity in the vital interests of data subjects (Article 6(1)(d)) or necessity for the performance of tasks carried out by public bodies (Article 6(1)(e)). Further, the right to objection does not apply where the controller can show "legitimate grounds" (rather than "*compelling* legitimate grounds") for continuing to process the data. Where an objection is upheld, the controller may still process the personal data to establish, exercise or defend legal claims (Article (19(1a)). The right to object to processing for direct marketing purposes is amended such that it no longer has to be free of charge (Article 19(2)).

The Irish Presidency proposes to maintain data portability as a separate right (Article 18), rather than subsuming it into the right of access (Article 15), as proposed by lead rapporteur Jan Phillip Albrecht.

The timeframe for responding to data subject requests under Articles 16 to 19 is extended from one month to up to a further two months, depending on the complexity and number of requests.

Routes to immediate judicial redress for data subjects are reduced, and the local data protection authority is reinstated as the primary contact for all data subject complaints (Article 12(3)).

Note

This Briefing Paper has been produced by the Hunton & Williams Privacy and Information Law Team for use by clients. If you would like to receive an electronic copy, please contact Bridget Treacy (btreacy@hunton.com), Wim Nauwelaerts (wnauwelaerts@hunton.com) or Rosemary Jay (rjay@hunton.com).

This Briefing Paper should be used as general guidance only and should not be relied upon as advice. If you require advice please speak to your usual contact at Hunton & Williams to discuss your needs. The material is intended to help your organisation start to prepare for the important changes that will occur in the field of data protection compliance. You are welcome to use it provided you credit Hunton & Williams using the copyright wording at the end and use is limited to within your organisation. If you know of anyone else who would find it useful, please feel free to pass our contact details to them and we will be happy to supply an electronic copy.

HUNTON& WILLIAMS

Executive Briefing Paper - Update

Proposed General Data Protection Regulation

Update 3
December 2013
European Parliament Compromise Text

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Hunton & Williams
30 St Mary Axe
London
EC3A 8EP
United Kingdom

Introduction

On January 25, 2012, the European Commission released its widely anticipated data protection legislative framework proposal, intended to replace Directive 95/46/EC. The Commission's proposal consists of two instruments: a general data protection regulation (the "Draft Regulation") and a directive on processing personal data in relation to police and criminal justice matters.

On October 21, 2013, the European Parliament approved its compromise text of the Draft Regulation (the "Compromise Text"). The approval of the text comes after months of negotiations between the various parliamentary committees and was led by the lead committee, the Committee on Civil Liberties, Justice and Home Affairs ("LIBE Committee").

The approval of the Compromise Text marks the next stage in the Draft Regulation's legislative journey. The next stage is for the Council of Ministers to reach an agreement on the Draft Regulation, after which a "trilogue" between the Parliament, the Council and the Commission will be established to agree on the final text. A vote is expected before the parliamentary elections in May 2014. The coming months are therefore likely to be a period of intense negotiations; businesses should therefore try to remain engaged in the discussions.

In this Update we have flagged those proposals which would likely have a significant impact if they were to be adopted. This Update follows the pattern of our Executive Briefing paper and previous two updates, and like those documents, can be used as a basis for internal briefings.

This Update is divided into the same nine sections as the Executive Briefing paper and previous updates:

1. Definitions
2. Scope
3. Data quality principles
4. Overseas transfers
5. Security
6. Supervisory authorities
7. Internal controls
8. Individual rights
9. Exemptions

Section 1 - Definitions

The Compromise Text proposes new definitions of "pseudonymous data", "encrypted data", "profiling" and "third party".

"Pseudonymous data" are defined as "personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution". Where the controller is unable to comply with the Draft Regulation because it is processing pseudonymous data, the controller is not obliged to comply with that particular provision of the Draft Regulation. Notably, the Albrecht Report proposed a new definition of "pseudonym" but not "pseudonymous data" and the Presidency's proposals introduced an additional category of "pseudonymised" data.

"Encrypted data" are defined as "personal data, which through technological protection measures is rendered unintelligible to any person who is not authorised to access it". The inclusion of this definition reflects the Parliament's desire for the Draft Regulation to create a privacy framework that is mindful of technical processes.

"Profiling" is defined as "any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour". This definition remains unchanged from the definition originally proposed by Rapporteur Albrecht in his draft report in January 2013 (*see* Update 1) and largely mirrors the definition provided in the Presidency's proposals.

"Third party" is defined as "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data". The "third party" concept is referred to in the lawfulness of processing provisions (*see* Section 3, below).

Additionally, a number of amendments to existing definitions are proposed:

- "Data subject" is amalgamated with "personal data", rather than separately defining "personal data" as any information relating to a data subject. This follows the approach recommended by the Irish Presidency of the Council (*see* Update 2). Rapporteur Albrecht's original draft report proposed amending "data subject" to introduce the concept of the ability to "single out" a natural person.
- "Personal data breach" is amended to clarify that a data breach does not only occur as a result of a security breach, but can also occur due to the accidental loss or disclosure of personal data. This retains the same amendment originally proposed by Albrecht in his draft report.
- "Genetic data" is expanded and to mean "personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained".
- The concept of a "main establishment" is clarified. The Compromise Text maintains the meaning of "main establishment" as the place of the establishment of the undertaking in the EU where the main decisions as to the purposes, conditions and means of the processing of personal data are taken. However, the Compromise Text specifies criteria for main establishment, including:
    - the location of the controller or processor's headquarters;
    - the location of the entity within a group of undertakings which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in the Draft Regulation; and
    - the location where effective and real management activities are exercised determining the data processing through stable arrangements.
- The "special categories of data" (sensitive personal data) are expanded to also include data revealing philosophical beliefs, sexual orientation or gender identity, biometric data, administrative sanctions and suspected offences.

Section 2 - Scope of the Draft Regulation

Under the Compromise Text, the extra-territorial scope of the Draft Regulation is made explicit. It applies to the processing of personal data in the context of the activities of a controller's or processor's establishment, even if the processing does not take place in the EU (e.g., where processing is actually conducted overseas or in the cloud). The Compromise Text greatly extends the territorial scope by making processors as well as to controllers established outside of the EU subject to the Draft Regulation, where the processing relates to offering goods or services to data subjects in the EU, or monitoring them. The extension of the territorial scope may cause ambiguity and confusion in two particular respects: the residency requirement for data subjects in the EU is deleted, as is the requirement of monitoring data subjects' *behaviour*. Under the first deletion, the Draft Regulation could apply to data subjects temporarily travelling in the EU. The second deletion makes it unclear what would constitute "monitoring" of data subjects. The Compromise Text also amends the application of the Draft Regulation by deleting the exemption for EU institutions, bodies, offices and agencies, a deletion which the Irish Presidency's compromise text also proposed.

The domestic processing exemption (i.e., by natural persons exclusively in the course of a personal or household activity) has also been expanded so that it shall also apply to the publication of personal data "where it can be reasonably expected that it will be only accessed by a limited number of persons". This would likely cover situations such as sharing holiday photographs to a group of people on an online shared. Recital 15 clarifies that the Draft Regulation should not apply to "processing of personal data by a natural person, which are exclusively personal, family-related, or domestic, such as correspondence and the holding of addresses or a private sale and without any connection with a professional or commercial activity".

Section 3 - Data Quality Principles

The Compromise Text allows for the processing of personal data where it is necessary for the purposes of the legitimate interests of the controller, or in the case of disclosure, the legitimate interests of the third party to whom the data are disclosed and which meet the reasonable expectations of the data subject, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This largely preserves the current position of legitimate interests under Directive 95/46/EC, in contrast to the amendments originally proposed by Albrecht that would have drastically restricted the legitimate interests basis for use in "exceptional circumstances" only. The amended recital gives some examples of processing which could be carried out under this ground. These include processing for the purpose of enforcement of legal claims or for postal direct marketing. The Compromise Text also amends the definition of consent to include purpose limitation; consent automatically loses its validity once the original purpose of the processing ceases to exist. Article 7 on consent is also amended such that data subjects cannot consent to processing activities which are partly (and presumably, wholly) in breach of the Regulation. In a further restriction, processing which would otherwise be incompatible with the purpose for which data are held cannot be legitimised by the data controller pointing to another legal ground on which to justify the processing.

Section 4 - Overseas Transfers

The general principle for transfers under Article 40 remains unchanged. Article 39 introduces "European Data Protection Seals" ("EDPSs"), which would enable certified organisations to rely on their privacy seals as an adequate basis for transfers of data outside the EEA. The introduction of EDPSs is essentially a certification programme whereby controllers and processors would be apply to have their data processing activities audited and certified by supervisory authorities or accredited third parties. There would be a publicly available electronic register listing valid (and "invalid") certificates.

A new provision dealing with transfers or disclosures not authorised by EU law has been inserted as Article 43(a). This provision prohibits the disclosure of personal data as ordered by a court, tribunal or administrative authority of a third country, unless an appropriate international agreement is in force. In such instances, the controller or processor and, if any, the controller's representative, would be required to obtain prior authorisation for the transfer or disclosure and to inform the data subject of the request and disclosure. This

provision appears to address fears surrounding foreign law enforcement access to data, following the recent PRISM revelations.

Section 5 - Security and Breach Notification

The definition of "personal data breach" is amended to clarify that a data breach can occur without a security breach (as per Albrecht's original proposals). Article 31 relaxes the data breach notification requirements. The 24-hour window to report a breach to the supervisory authority is deleted and no timing is specified; rather breaches must be reported "without undue delay". In contrast, both Albrecht's draft report and the Irish Presidency's proposals extended the timeframe for reporting personal data breaches from 24 hours to 72 hours.

Section 6 - Powers of Supervisory Authorities and the Commission

Each supervisory authority would oversee the processing operations which take place on the territory of its state and processing operations outside its own territory relating to the processing of the personal data of its residents. An authority could therefore supervise processing outside its jurisdiction and some data controllers and data processors would be subject to the supervision of more than one authority.
The concept of a "lead authority" is unchanged; if a controller or processor is established in several countries in the EU the lead authority would remain the authority for the country in which the controller or processor has a main establishment. Its role, however, has been extended. This is in contrast to Albrecht's original proposals which drastically reduced the role of the lead authority.

There is guidance on how the main establishment is to be selected. Where it is not clear where the main establishment is situated or there is disagreement between supervisory authorities or where the controller or processor is outside the EU but processes personal data on individuals in several countries the European Data Protection Board may issue an Opinion on which supervisory authority should take the lead.

Recital 92 requires that a supervisory authority must have "adequate financial and personal resources to fully carry out its role, taking into account the size of the population and the amount of personal data processing". This may have been addressed to allay the fears of some data protection authorities, such as the ICO, that without the notification framework supervisory authorities would have no obvious source of funding.

Article 79 of the Compromise Text increases the potential fines to 5% of annual worldwide turnover of an enterprise or €100m, whichever is greater.

As noted in relation to transfers, Article 39 develops the concept of the European Data Protection Seal (EDPS) under which controllers and processors would be apply to have their data processing activities audited and certified by supervisory authorities or third parties accredited by supervisory authorities. In the event of a violation of the Draft Regulation, a fine would only be imposed on companies holding a valid EDPS if the violation was intentional or negligent.

Article 77 of the Draft Regulation includes the right for a person who has suffered damage as a result of a breach of the Draft Regulation to claim compensation. The European Parliament extends the damage to include non-pecuniary damage. It also requires that the default position, where there is more than one controller or processor involved in the processing, is that each controller or processor will be jointly and severally liable for the damage (unless they have an appropriate written agreement establishing liability in the determination of their responsibilities).

Section 7 - Prior Notice to Supervisory Authorities and Internal Controls

The Commission draft of January 2012 replaced the system of notification to supervisory authorities with a system of internal record keeping by controllers, processors and representatives. The Compromise Text's

proposals reflect the same approach but the list of documentation particulars is far shorter, limited to only name and contact details of the controller or joint-controller, a data protection officer or controllers to whom personal data are disclosed. In contrast, Albrecht's original draft report proposed to replace the internal records, at least for data controllers, with personalised notifications to data subjects.

The provisions on accountability and responsibility of controllers in Article 22 are extended. They now include a requirement on controllers which are required to produce any regular general reports, such as the annual reports of publicly traded companies, to include a summary of their data protection compliance policies and measures in such reports.

Under the Compromise Text, Data Protection Impact Assessments ("DPIAs") form part of the "Lifecycle Data Protection Management" provisions under Chapter IV, section 3. The obligation to conduct a DPIA is tied in with a new provision inserted in the Compromise Text, Article 32a ('Respect to Risk'). If certain processing operations are likely to present specific risks (e.g., processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period or processing special categories of personal data, location data or data on children or employees in large scale filing systems), the controller or processor must carry out a DPIA. Article 33 states that an assessment carried out as part of a DPIA "shall have regard to the entire lifecycle management of personal data from collection to processing to deletion" and at a maximum period of two years from the date a DPIA is conducted, a compliance review must be undertaken (Article 33a).

As in the Albrecht's original proposals, the Compromise Text alters the threshold for the appointment of a data protection officer ("DPO") so that it relates to the number of affected data subjects rather than the number of staff the controller or processor employs. Article 35 provides that a controller or processor must appoint a DPO where processing personal data in relation to more than 5,000 data subjects in any consecutive 12 month period, or where the core processing activities relate to processing sensitive personal data, location data, children's data, or employees in large scale filing systems. The minimum protected tenure of DPOs is extended from two years to four years. A group of companies may appoint a primary DPO, provided the DPO is easily accessible from each place of establishment.

Section 8 - Individual Rights and Remedies

A new Article 13a has been inserted which requires controllers to provide standardised information to data subjects, including whether personal data are collected "beyond the minimum necessary for each specific purpose of the processing", "retained beyond the minimum necessary for each specific purpose of the processing", "processed for purposes other than the purposes for which they were collected" or sold to third parties, and the general notice requirements under Article 14 are also extended. This contrasts the Irish Presidency's compromise text, which proposed greatly reducing the lengthy list of notice requirements to two key requirements: (i) the identity of the data controller; and (ii) the purpose(s) of the processing of their personal data. The information listed in Article 13a would have be represented in a standardised tabular format, using text and symbols to depict the relevant particulars.

The Compromise Text also requires the controller to provide notice to individuals where personal data was provided to public authorities within the preceding 12 months. Article 14(1)(ha) does not specify that the controller must have handed over the personal data to the authorities, nor does it include any other circumstances or details. A similar provision requires controllers to provide similar notice in response to a subject access request. Amendments to the notice provisions may reflect recent sensitivities regarding law enforcement access to data following the PRISM scandal.

Profiling that has a discriminatory effect on the grounds of race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, sexual orientation or gender identity is prohibited outright, and the controller must implement safeguards against possible discrimination resulting from profiling.
In addition to the Article 13a particulars to be provided by the controller to the data subject in the Compromise Text, the controller must also provide the data subject with the identity and contact details of the controller or the DPO (Article 14(1)(a)), the purposes of the processing for which the personal data are intended, as well as information regarding the security of the processing of personal data (Article 14(1)(b)) and the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period (Article 14(1)(c)).

In addition to the introduction of a specific definition of "profiling", at Article 14 under the notice requirements, controllers must provide notice to individuals with regard to their right to object to profiling. Recital 58(a) provides state that "profiling based solely on the processing of pseudonymous data should be presumed not to significantly affect the interests, rights or freedoms of the data subject". Where profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous.

According to Article 17 of the Compromise Text, any data subject should also have the right to have his or her personal data erased upon request. To bolster this right, if the data has been made public by the controller without justification and a data subject asks a controller (e.g., an Internet company) to erase his or her data, the company should also forward the request to other companies that maintain the same data on the individual. This "right to erasure" replaces the "right to be forgotten" that was initially proposed by the European Commission.

The Compromise Text places the right to data portability in the subject access provisions at Art 15(2a) but the right is largely unchanged and, Recital 51a states that "data controllers should be encouraged to develop interoperable formats that enable data portability".

Section 9 - Exemptions and Exceptions

The exemption for freedom of expression specifically references that right (rather than referring to journalism) and the rights in the EU Charter of Fundamental Rights.

Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the consent may be given for one or more specific and similar researches (Article 81(1)). This provision of consent being given for multiple 'researches' is not provided in the Albrecht Report nor the Presidency's proposals.

The special provisions for the processing of personal data in the context of employment are significantly extended. Member States may set special rules for the processing of personal data in connection with employment. Article 82 sets out in detail the minimum standards which must be included in such provisions. These include specific rules on monitoring and surveillance, including email and telephone monitoring as well as banning the use of "blacklists" in the employment context.

Note

This Briefing Paper has been produced by the Hunton & Williams Privacy and Information Law Team for use by clients. If you would like to receive an electronic copy, please contact Bridget Treacy (btreacy@hunton.com), Wim Nauwelaerts (wnauwelaerts@hunton.com) or Rosemary Jay (rjay@hunton.com).

This Briefing Paper should be used as general guidance only and should not be relied upon as advice. If you require advice please speak to your usual contact at Hunton & Williams to discuss your needs. The material is intended to help your organisation start to prepare for the important changes that will occur in the field of data protection compliance. You are welcome to use it provided you credit Hunton & Williams using the copyright wording at the end and use is limited to within your organisation. If you know of anyone else who would find it useful, please feel free to pass our contact details to them and we will be happy to supply an electronic copy.

About Hunton & Williams

Hunton & Williams is a full-service international law firm of more than 800 attorneys. The firm's 19 offices in Europe, Asia and the United States serve clients around the world. Hunton & Williams has been recognised as the top law firm globally for privacy and data security by *Computerworld* magazine, as well as Chambers and Partners and The Legal 500.

European Data Protection and Privacy Practice

Our integrated data protection team offers assistance on all aspects of European data protection law, and is led by internationally recognised partners Bridget Treacy and Wim Nauwelaerts in the firm's London and Brussels offices, respectively.

We have extensive experience organising, managing and coordinating compliance projects with both national and international dimensions, allowing our clients to efficiently manage their multijurisdictional needs. We provide counsel on a wide range of areas, including:

- Assisting with **data breach** notification requirements, including mitigating and managing the risks arising from data breaches and the management of reputation;
- Creating strategies for **international data transfers**, including BCRs, safe harbor clauses and model clauses;
- Advising on the compliance issues raised by **cloud-based data processing** services;
- Addressing challenges raised by **social networking services** and related technologies, for both providers and corporate users;
- Advising on the **use of cookies** and the compliance challenges posed by the amended e-Privacy Directive;
- Advising on the cross-border implementation of **employee monitoring and whistle-blowing** schemes;
- Addressing data protection issues in the context of outsourced arrangements, particularly concerning **global HR databases**;
- Developing tailored **compliance tools and procedures** (such as privacy impact assessments, checklists, notice and consent forms, sample security procedures); and
- Working with senior management to develop comprehensive **information governance strategies** that assist in managing risk and encouraging innovation.

Lawyers in our Brussels and London offices are fluent in many European languages, and they have studied law or been admitted to practice in several jurisdictions, including Belgium, France, Germany and the UK. Our European attorneys are often assisted on projects by our privacy lawyers in our Asian and US offices.

We have established a network of specialised privacy and data protection lawyers in Europe and beyond, with whom we often work on projects. This approach allows us to call on the services of highly knowledgeable privacy law specialists from all over the world, while coordinating the work so that our clients deal with only a single point of contact.

Augmenting our core data protection and privacy practice is the Centre for Information Policy Leadership, a privacy think tank associated with the law firm. The Centre provides strategic consulting services and is a forum for developing privacy solutions. The Centre brings together companies, consumer leaders and senior policymakers to develop next-generation privacy principles to facilitate global, digital information flows.

Our data protection lawyers maintain strong relationships with officials at the European Commission, national data protection authorities, the Article 29 Working Party and the European Data Protection Supervisor. Our team is closely involved in policy discussions underpinning the review of the European Data Protection Directive, and our views are frequently sought by legislators and policy makers. Our team has successfully led negotiations with European data protection authorities and the Commission, and have close ties to international organisations such as the Council of Europe and the OECD.