ALERT MEMORANDUM

The General Data Protection Regulation: Key Changes and Implications

May 13, 2016

On April 14, 2016, the European Parliament formally approved the General Data Protection Regulation (the "**GDPR**") proposed by the European Commission (the "**Commission**") in January 2012. This formal approval follows the compromise agreement reached with the Council of the European Union in December 2015 and the Council's adoption of its position at first reading on April 8, 2016. The GDPR was published in the Official Journal of the European Union on May 4, 2016 and will come into force on May 24, 2016. There will then be a two-year transition period ending on May 25, 2018, at the end of which businesses will need to be fully compliant with the GDPR.

The GDPR replaces the current EU Data Protection Directive 95/46/EC (the "**DPD**") with a view to enhance existing legal requirements, create new rules and set out significant fines for organizations failing to comply. The GDPR aims to introduce a more harmonized approach to data protection across the EU and to remove inconsistencies between national data protection regimes. Transitioning to the new regulation will require effort on the part of organizations falling under its jurisdiction, which can also include organizations established outside the EU where such organizations process data belonging to EU residents. The GDPR imposes stringent obligations on data controllers *as well as processors* and grants broad enforcement powers to supervisory authorities. Businesses that do not comply with the GDPR may face fines of up to *4% of their global revenue or EUR 20,000,000, whichever is higher*. Consequently, organizations will have to look closely at their current data protection policies and make any necessary changes. This alert memorandum covers some of the key changes introduced by the GDPR and suggests practical approaches to potential change requirements.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

LONDON
City Place House
55 Basinghall Street
London EC2V 5EH, England
T: +44 20 7614 2200

Colin Pearson
+44 20 7614 2390
cpearson@cgsh.com
David Toube
+44 20 7614 2384
dtoube@cgsh.com
Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

PARIS
12, rue de Tilsitt
75008 Paris, France
T: +33 1 40 74 68 00

Fabrice Baumgartner
+33 1 40 74 68 53
fbaumgartner@cgsh.com
Emmanuel Ronco
+33 1 40 74 69 06
eronco@cgsh.com

ROME
Piazza di Spagna 15
00187 Rome, Italy
T: +39 06 69 52 21

Francesco de Biasi
+39 06 6952 2254
fdebiasi@cgsh.com

BRUSSELS
Rue de la Loi 57
1040 Brussels, Belgium
T: +32 2 287 2000

Christopher Cook
+32 22872137
ccook@cgsh.com
Natascha Gerlach
+32 2 287 2201
ngerlach@cgsh.com

FRANKFURT
Main Tower
Neue Mainzer Strasse 52
60311 Frankfurt am Main, Germany
T: +49 69 97103 0

Thomas Kopp
+49 69 97103 246
tkopp@cgsh.com

I. Application and Implementation of the GDPR[1]

Increased harmonization. The GDPR is structured as a regulation rather than as a directive and consequently will, for the most part, not require implementation in each of the member states of the EU (the "**Member States**"). The motivation was to provide organizations with a single, consistent set of data protection rules, rather than to risk the inconsistency of application that would arise as a result of varying implementing acts in each Member State.

Additionally, a new "*consistency mechanism*" will require supervisory authorities[2] to cooperate more closely with each other, and, where relevant, the Commission is to ensure consistent application of the GDPR (Article 63).

The GDPR also introduces a "*One-Stop Shop*" mechanism; the One-Stop Shop is designed to allow controllers[3] and processors[4] established in multiple Member States to deal with one supervisory authority only. The supervisory authority of the *main establishment* of the controller or processor will be competent to act as the "*lead*" supervisory authority for cross-border processing, while other Member States' supervisory authorities will be competent for complaints affecting data subjects or establishments in that Member State (Article 56).

However, inconsistencies in application between Member States will remain. The GDPR allows Member States to introduce specific conditions for certain data processing activities, such as the processing of national identification numbers (Article 87), the age for valid consent (Article 8),[5] data processing by controllers or processors that are subject to an obligation of professional secrecy (Article 90) and exemptions for the right to freedom of expression and information, including processing for journalistic, academic or artistic purposes or literary expression (Article 85). Critically, data processing in the employment context (Article 88), an issue of great importance for multinational players, has also received such a national carve out.

Key practical points to consider:

- Businesses should identify their "*lead*" supervisory authority.
- Businesses should monitor any further guidance provided by the supervisory authorities on the interpretation of the GDPR and any upcoming changes to the existing data protection law, including the implementation of any national carve outs.

Expanded territorial scope. Under the DPD, EU data protection rules apply (1) to processing carried out in the context of the activities of an establishment of the controller on the territory of a Member State, and (2) where the controller is not established on EU territory, but the processing takes place using equipment situated on the territory of a Member State (unless it is merely used for transit). However, the case law of the Court of Justice of the European Union (the "**CJEU**") has expanded the concept of "*establishment*".[6] In *Google Spain*, the CJEU considered whether an establishment within the EU (Google Spain) was processing personal data for the purposes of the DPD, where the processing took place "*in the context of the activities*" of its US parent company, but was not carried out by the establishment in the EU, itself. The CJEU concluded that the DPD was applicable and held that the activities of a parent company and its subsidiary will be inextricably linked if the subsidiary exists to make the parent company economically profitable. This broadening of the principle of establishment has been carried over into the GDPR. The GDPR provides that: (1) personal data processed in the context of the activities of an establishment of a controller or a *processor* in the EU will fall within the scope of the legislation (Article 3(1)); and (2) the processing of EU data subjects' personal data by a controller *not* established in the EU, *where the processing activities are related to the offering of goods or services to the relevant data subject or the monitoring of the data*

[1] References to articles and recitals are to the GDPR unless stated otherwise.

[2] Article 51 of the GDPR requires that each Member State provides for one or more independent public authorities to be responsible for monitoring the application of the GDPR (the supervisory authorities).

[3] A "*controller*" is a body that, alone or jointly with others, determines the purposes and means of processing of personal data (Article 4(7)). Therefore, companies will be "*controllers*" where they collect, keep and use (i.e. control and are responsible for) personal information on a computer or in structured manual files about living people. This definition is unchanged from the DPD.

[4] A "*processor*" is a body which processes personal data on behalf of a controller (Article 4(8)). A company will be a "*processor*" where it holds or processes personal data but does not exercise responsibility for or control over the personal data. Typical examples of processors include payroll companies, accountants and market research companies. This definition is unchanged from the DPD.

[5] Member States may provide for a lower age (i.e., lower than 16 years old) for valid consent in relation to the processing of the personal data of a child, provided that the lower age is not below 13 years.

[6] Case C131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos* ("*Google Spain*"). See also Case C230/14 *Weltimmo v Nemzeti Adatvédelmi és Információszabadság Hatóság*.

subjects' behavior in the EU, will also be caught (Article 3(2)). A nexus will be established based on the location of the data subjects to which the relevant activities are targeted, not the act of processing; the company undertaking the processing does not need to have a presence in the EU. The scope of the GDPR makes the location of the data subject key to the determination of the regulation's territorial reach.

The GDPR also provides that where a controller or processor is not established in the EU, it must designate, in writing, a representative in the EU. However, a representative will not be required where the processing activities of the controller or processor are occasional, do not include processing of special categories of data[7] on a large scale and such processing is unlikely to result in a risk to the rights and freedoms of natural persons taking into account the nature, context, scope and purpose of the processing (Article 27).[8]

Consequently, entities established outside of the EU, that are not currently subject to the DPD, may find themselves subject to the GDPR when it comes into force.

Key practical points to consider:

- Businesses should be aware that there is no need to have a presence in the EU for nexus to be established. The territorial reach of the GDPR will be driven by the location of the data subject.
- Businesses established outside of the EU should assess whether they are processing personal data of individuals who are located in the EU and whether these processing activities relate to the offering of goods and services to the data subject or the monitoring of the data subject's behavior in the EU.

II. Obligations Placed on Controllers and Processors

Liability for data processors. In contrast to the previous rules under the DPD, the GDPR introduces statutory obligations on processors.[9] Failure to comply will result in liability similar to that of a controller. Processors now face direct liability; for example, where both a controller and a processor are involved in the same processing activities and are responsible for any damage caused, each of the controller and the processor can be liable for the entire damage (Article 82(4)). In addition**,** a processor's responsibilities under the GDPR are considerably more extensive than those contained in the DPD. For example, processors must maintain written records of their processing activities (Article 30(2)); in certain circumstances, processors will have to appoint a data protection officer (Article 37); processors will be statutorily required to implement technical and organizational measures to ensure data security (Article 32); and they will have to notify the controller of all data breaches (Article 33(2)).

Key practical points to consider:

- As a result of the additional obligations and the direct liability regime imposed under the GDPR, data processors and controllers should expect to engage in detailed negotiations of data processing agreements.
- Processors will want to ensure, now more than ever, that the scope of a controller's instructions are clear, that consent has been properly obtained from data subjects and that limitation of liability and indemnity measures exist to protect their position.

Consent. Under the GDPR, consent as a legal basis for processing will be more difficult to obtain. The burden of proof for valid consent explicitly remains on the controller who relies on this as a legal basis for processing (Article 7(1)). Consent must be freely given, specific, informed and *unambiguous*. As consent has to be *actively* given, "*silence, pre-ticked boxes or inactivity*" would not constitute consent.[10] The GDPR provides a specific example of where consent would not be considered as having been freely given: where the performance of a contract is made conditional on consent to processing of personal data that is not necessary for the performance of such a

[7] This would include, health data, biometric and genetic data, but also processing of data relating to criminal offences and convictions, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union memberships (Article 9).

[8] A representative will also not be required where the controller or processor is a public body.

[9] Under the DPD, statutory obligations fall solely upon the controller. The DPD requires that processing must be governed by a contract between the processor and the controller, which clearly sets out the obligations of the processor. Therefore, under the DPD regime, only *contractual* obligations are imposed on processors.

[10] Recital 32

contract (Article 7(4)). Additionally, consent must be specific and clearly distinguishable from any other associated matters.[11]

Key practical points to consider:

- Businesses should review their data flows and audit the legal basis on which they process personal data. Businesses may want to explore whether they can rely on grounds, other than consent, for lawful data processing (such as "*necessary for the performance of a contract to which the data subject is a party*" or for the purposes of legitimate interests). See Article 6(1) for the full list of lawful data processing grounds.
- Businesses will need to assess and update their consent forms and documentation, where applicable.

Accountability. The GDPR no longer requires registration with a supervisory authority. Instead, controllers and processors have a general accountability obligation to implement appropriate technical and organizational measures to be able to demonstrate that processing is performed in accordance with the GDPR.

Technical and organizational measures include the following:

- Record keeping. Controllers and processors must maintain records of processing activities (Article 30).
- Data protection officer. Controllers and processors must designate a data protection officer where necessary as the result of the scale of their processing of personal data (including sensitive data) or where required by EU or a Member State law (Article 37). Previously, the role of data protection officers focused on the internal application of national laws implementing the DPD. Under the GDPR, data protection officers are actively required to *monitor* compliance with the GDPR (Article 39).
- Impact assessment. Controllers must carry out an impact assessment of the envisaged processing operations where the processing activities are likely to result in a high risk to the rights and freedoms of natural persons (Article 35).
- Data protection by design / Data protection by default. Controllers will need to ensure that data protection requirements are taken into account when putting into place the means for processing data (Article 25). Additionally, controllers must implement technical and organizational measures to ensure that, by default, only personal data that is necessary for the specific activity undertaken is processed and retained (i.e., data protection by default). Businesses will need to plan future product strategies bearing in mind the GDPR requirements (i.e., data protection by design).[12]
- Notification of data breaches. In the event of a personal data breach, controllers must notify the relevant supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach (Article 33(1)).[13] Processors must also notify the controller without undue delay after becoming aware of such breach (Article 33(2)). Where the breach is likely to result in a high risk to individuals' rights and freedoms, controllers must communicate the data protection breach to the individuals concerned, subject to limited exceptions (Article 34(1)).[14]

Key practical points to consider:

- Businesses will need to review their existing compliance programs and ensure that these are updated as necessary to comply with the GDPR.
- Businesses will need to develop policies and an effective response plan for data breaches. Since the GDPR harmonizes data protection requirements across the EU, multinational businesses will be able to implement one Europe-wide set of policies and response plans.
- Businesses will need to devote additional resources in order to comply with the reporting obligations.

[11] Recital 32 and Article 7

[12] Recital 78

[13] Notification will not be necessary where the breach is unlikely to result in a risk to individuals' rights and freedoms.

[14] These exceptions include where (a) the controller has implemented appropriate technical and organizational protection measures and those measures were applied to the personal data affected by the breach, (b) the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize and (c) notifications to the individuals concerned would be disproportionate. In this case, the controller must instead make a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

- Businesses will need to train their data protection officers and ensure they understand their obligations.
- Businesses will need to ensure data processing and retention is limited to the extent strictly necessary.
- Data protection will need to be at the forefront of any new service or product development plans.
- Businesses will need to conduct risk and impact assessments in relation to high-risk processing activities.

III. Enforcement and Remedies

Increased enforcement powers. The GDPR grants broad and harmonized powers to the supervisory authorities, including the ability to impose higher fines for violations of: (1) up to the higher of EUR 20 million or 4% of the total worldwide annual turnover (revenue) of a company for infringements of the requirements relating to the basic principles for processing (including conditions for consent),[15] certain data subjects' rights[16] and transfers of personal data to a recipient outside the European Economic Area ("**EEA**")[17] and (2) up to the higher of EUR 10 million or 2% of the total worldwide annual turnover (revenue) of a company for infringements of certain requirements such as various obligations of controllers and processors[18] (Article 83). By comparison, current fines under national laws are relatively low. For example, the maximum fine in the UK under the *Data Protection Act 1998* is GBP 500,000 and the maximum administrative fine in France under the *Loi Informatique et Libertés* is EUR 150,000 (which may be doubled in case of a repeated breach).

Investigative powers. The GDPR grants investigative powers to supervisory authorities. A supervisory authority will be able, for example, to order controllers or processors to provide information the supervisory authority requires in order to perform its tasks, carry out investigations in the form of data protection audits and to obtain access to the premises of controllers and processors in certain circumstances (Article 58). Supervisory authorities will in turn have to prepare for this new role and will require the necessary budget from their respective Member States.

Key practical point to consider:

- Businesses will need to conduct a risk analysis of non-compliance in light of the new requirements under the GDPR.

European Data Protection Board. The GDPR introduces a new European Data Protection Board (the "**EDPB**") (Article 68). The EDPB will replace the current Article 29 Working Party.[19] [20] The EDPB will be responsible for ensuring the consistent application of the GDPR and as such will monitor the application of the GDPR and issue guidelines, recommendations and best practices on various matters under the GDPR (Article 70).

IV. Rights of Data Subjects under the GDPR

Extended rights for data subjects. While the current rights of access (Article 15), rectification (Article 16), to object (Article 21) and to lodge complaints (Article 77) remain largely the same, the GDPR introduces additional rights for data subjects. These additional rights include:

- Right to be forgotten. The GDPR now formally establishes a qualified right to erasure, commonly referred to as the "*right to be forgotten*". Data subjects will have the right to require the controller to erase his or her personal data, for example, where: (1) the retention of the personal data is no longer necessary, (2) the data subject objects, (3) there is no overriding, countervailing interest or (4) the data subject withdraws consent (Article 17). There are a number of derogations to this right, such as where personal data is processed for scientific or historical research purposes or statistical purposes or in relation to a legal claim (Article 17(3)).
- Right to data portability. The GDPR provides data subjects with the right to (1) receive their personal data in a structured, commonly used and machine-readable format (such that the personal data can be easily transferred to another controller)

[15] Pursuant to Articles 5, 6, 7 and 9
[16] Pursuant to Articles 12 to 22
[17] Pursuant to Articles 44 to 49
[18] Pursuant to Articles 8, 11, 25 to 39, 42 and 43

[19] The Article 29 Working Party is set up under Article 29 of the DPD. It has advisory status and acts independently. It provides non-binding guidance on the interpretation of the DPD by issuing opinions and recommendations.
[20] Recital 139

and (2) transfer this data to another controller (Article 20).

- Right to object to profiling. The data subject has the right not to be subject to automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her (Article 22).[21] Profiling is defined to include any form of automated processing of personal data; in particular, where data processing is used to analyze or predict aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements (Article 4(4)). Profiling, therefore, includes most forms of online tracking.
- Further information to be provided where personal data is obtained from data subjects. Under the GDPR, data subjects are entitled to receive extensive information when personal information is collected from them (including details of the purpose of the data processing, retention periods, identity and contact details of the controller, logic of any profiling, the safeguards adopted for international transfers and details of their rights to lodge complaints with supervisory authorities) (Article 13).

Key practical points to consider:

- Businesses must consider early how they will handle data subjects exercising their rights under the GDPR.
- Businesses may want to re-evaluate their procedures and policies on collecting and storing personal information.
- Businesses who rely on profiling activities, such as for online advertising and in connection with social media, will need to consider implementing appropriate consent mechanisms.
- Businesses will need to devote additional resources to implement systems and controls in order to ensure they can easily track the personal data, extract it and provide it to individuals in the required format.
- Often the deletion of personal data can be challenging. Businesses will need to devote additional resources to implement effective systems and controls in order to give effect to the right to be forgotten.

V. Cross-border Data Transfers

The GDPR maintains the principle that transfers of personal data to third countries must take place only to the extent that an adequate level of protection for the personal data can be ensured. The GDPR lays out the following data transfer conditions, which largely mirror the position under the DPD:

- Adequacy decisions. Transfers of personal data outside the EU will be allowed where the Commission has issued an adequacy decision asserting that the third country provides an adequate level of protection (Article 45(1)). The GDPR provides that adequacy decisions issued under the DPD *will* remain in force (Article 45(9)). However, when assessing the adequacy of the level of protection, the GDPR includes new criteria for the assessment of national security laws in the third country. Notably, the Commission must have regard to whether public authorities in such third countries may have access to personal data. The GDPR further provides that a third country must offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the EU (Article 45(2)). There have been growing concerns about access to personal data transferred to third counties by governments and public authorities reflected prominently in the recent CJEU decision of *Maximillian Schrems v Data Protection Commissioner ("Schrems")*,[22] which invalidated Commission Decision 2000/520/EC (commonly known as the EU-US Safe Harbor Decision), one of the most well-known adequacy decisions.
- Standard Contractual Clauses. Under the GDPR, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards. These appropriate safeguards include standard data protection clauses adopted by the Commission or by a supervisory authority and approved by the Commission (Article 46(2)). Where contractual clauses were authorized under the DPD as providing appropriate safeguards for the transfer of

[21] Exceptions to this include where the profiling is necessary for entering into or the performance of a contract between the data subject and controller, is authorized by EU or a Member State law to which the controller is subject or is based on the data subject's explicit consent.

[22] (Case C-362/14) [2015] EUECJ C-362/14

personal data to a third country, the GDPR provides that these authorizations will remain valid until amended, replaced or repealed (Article 46(5)).

- Binding Corporate Rules. The GDPR now formally recognizes "*Binding Corporate Rules*" as an appropriate safeguard for intra-group personal data transfers to third countries (Article 46(2)). Binding Corporate Rules are data protection policies adhered to by a controller or processor established in a Member State where it transfers personal data to a controller or processor in a third country within the same group of undertakings (Article 4(20)). The Article 29 Working Party has issued a number of recommendations over the years relating to Binding Corporate Rules, which may still be relevant to controllers and processors.[23] It remains to be seen how the Article 29 Working Party work product will be integrated by the EDPB.
- New Ground for Transfer of Personal Data Outside the EEA. Article 49 of the GDPR provides similar derogations, vis-à-vis transfers to third countries, to those listed in Article 26 of the DPD. For example, these derogations include:
  - explicit consent to the transfer by the data subject;
  - where the transfer is necessary in order to protect the vital interests of the data subject or of other persons;
  - where the transfer is necessary for the conclusion or performance of a contract in the interest of the data subject;
  - where the transfer is necessary for reasons of public interest; or
  - where the transfer is necessary for the establishment, exercise or defense of a legal claim.

  However, the GDPR adds to this list transfers that are "*necessary for compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject*" (Article 49(1)). This is restricted by the requirement that such transfers are not repetitive and concern only a limited number of data subjects. The GDPR also states that the controller must have provided suitable safeguards for the protection of personal data when such "*legitimate interest*" transfers occur and that the controller must inform both the supervisory authority and the concerned data subjects of the transfer. This additional derogation is welcome for companies who may need to transfer personal data in exceptional circumstances. However, it is unclear how this approach will work in practice given the lack of guidance on the suitable safeguards required and the need to inform the relevant supervisory authorities of transfers made pursuant to this derogation.
- Judgments of foreign courts and decisions of foreign administrative authorities. The GDPR provides that any judgment of a court or tribunal and any decision of an administrative authority of a third country that requires a controller or processor to transfer personal data will only be recognized if it is based on an international agreement, such as a mutual legal assistance treaty, in force between the third country and the EEA or a Member State (Article 48). This requirement may be difficult to apply in practice, because such agreements will not exist for all Member States and often only for criminal and not civil enforcement. The United Kingdom has already decided, in a written statement dated February 4, 2016, not to exercise its opt-in power under Protocol 21 of the Treaty of the Functioning of the European Union with respect to Article 48.[24] In its statement, the UK parliament indicated that such a decision was taken as a result of concerns relating to the integrity of the UK legal system. This may lead to inconsistencies in the application of the GDPR between Member States.

  Additionally, Article 48 is "*without prejudice to other grounds for transfer*" of personal data to countries outside the EEA and it is not clear yet how this interplays with the derogation relating to necessary transfers for the establishment, exercise or defense of legal claims (Article 49(1)(e)). More guidance from the EDPB is required.

Key practical points to consider:

- The GDPR provides an opportunity for businesses to re-consider how they handle international data transfers. This is not a new issue, but the consequences of non-compliance could be significant given the high fines contemplated by the GDPR.

[23] See, for example, Working Document WP 74, which sets out the main requirements in relation to the content of the Binding Corporate rules and Working Document WP 204, which sets out the context in which Binding Corporate Rules can be used.

[24] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2016-02-04/HLWS500/

- The GDPR includes useful provisions for intra-group transfers of personal data such as the Binding Corporate Rules and the Standard Contractual Clauses.
- Businesses should monitor any subsequent guidelines published on these to see how they will be treated by EU authorities especially post-*Schrems*.
- The "*legitimate interest*" derogation is a welcome addition. However, businesses should be careful when using this derogation given the uncertainties outlined above.

The GDPR adopts a risk-based approach to compliance. Companies engaged in processing personal data will be responsible for assessing the degree of risk that their processing activities pose to data subjects and for implementing necessary safeguards. As described above, the GDPR includes a new accountability principle, a requirement to maintain records and requires businesses to appoint a data protection officer, among other security requirements. In order to prepare for the GDPR's entry into force in 2018, companies should conduct an audit of their existing systems and processes to determine whether changes to their compliance practices need to be made. Non-compliance with the new requirements of the GDPR may lead to significant fines.

…

CLEARY GOTTLIEB