Milbank

18 APRIL, 2016

CONTACTS

Joel Harrison
Partner
+44-20-7615-3051
jharrison@milbank.com

Laurence Jacobs
Partner
+44-20-7615-3096
ljacobs@milbank.com

Sean Keaton
Partner
+44-20-7615-3078
skeaton@milbank.com

Nicholas Smith
Partner
+1-212-530-5275
nsmith@milbank.com

Data Privacy and Information Security Group Client Alert:
European Parliament Adopts EU General Data Protection Regulation (GDPR)

BACKGROUND

On April 14, 2016, the European Parliament adopted the new General Data Protection Regulation (**GDPR**). GDPR aims to create a more consistent data protection regime across the EU, by replacing the current Data Protection Directive (which is implemented and enforced differently in EU Member States) with a single, EU-wide Regulation. It also expands the geographic scope of EU data protection law, imposes a number of new obligations on data controllers and their service providers, creates new rights for individuals and includes a regime of significant fines (up to 4% of worldwide turnover) for compliance failures.

GDPR will be published in the Official Journal of the European Union shortly, and will enter into force 20 days later. Businesses will then have two years to comply with its requirements. This briefing note summarises some of GDPR's most important provisions and key next steps for organisations subject to GDPR's requirements.

KEY POINTS

1. **Direct obligations for data processors.** GDPR imposes obligations directly on data processors as well as on controllers. For example, processors are required to implement security measures and notify data breaches to controllers, to co-operate with supervisory authorities and in some cases to appoint their own data protection officers. Processors may also be liable to pay damages and fines for contraventions of GDPR.

2. **Greatly expanded geographic scope.** In addition to applying to data controllers and processors established in the EU, GDPR will also apply to data controllers and processors *that are not established in the EU* if they process personal data in relation to offering goods or services to individuals in the EU, or

if they monitor the behaviour of individuals in the EU. Any such controller or processor will be required to appoint an EU representative.

3. **Revised definition of personal data.** GDPR makes clear that information is treated as personal data whenever individuals can be identified by online identifiers, location data or identification numbers. Whilst some supervisory authorities already take this approach under the current Directive, the change in emphasis means that a number of organisations – particularly online service providers – will need to re-evaluate the extent to which they hold and process personal data.

4. **Much higher standard for consent.** Under GDPR consent must be *unambiguous* and be communicated by a *statement or clear affirmative action*. GDPR makes clear that inactivity, silence and pre-ticked boxes cannot constitute consent. Data subjects also have the right to withdraw consent at any time, and it must be as easy for them to do this as it was to give consent in the first place. GDPR also requires any written declaration to be *clearly distinguishable* from other matters (e.g. website terms or privacy policies).

   Consent must be freely given; in assessing this, particular account is taken of whether the performance of a contract is made conditional on giving consent to data processing that is unnecessary for the contract itself.

   In the context of online services, consent is not valid in relation to the processing of data about a child under 16 (Member States can lower this as far as 13) unless given by a person with parental responsibility.

   In addition to the new requirements for consent, GDPR imposes additional transparency obligations on data controllers, covering both the types of information that must be provided to data subjects about how their data is processed and the manner in which that information must be presented.

5. **New and enhanced rights for data subjects.** Individuals have a number of new and enhanced rights under GDPR, including the 'right to be forgotten' (i.e. the right to have data erased), the right to object to data processing (including profiling) on various grounds, and a new 'right to data portability' (i.e. the right to transfer personal data to other organisations).

6. **Requirements for profiling.** GDPR imposes restrictions on data controllers taking any decision about an individual based solely on automated processing of data (including automated evaluation of the individual's characteristics), if the decision *produces legal effects* concerning the individual or *significantly affects* the individual in a similar way. This will be permitted only with the individual's

explicit consent, where necessary for a contract with the individual or where authorised by EU or Member State law.

7. **Potential for significant fines.** Data controllers and processors can be fined up to *4% of total worldwide global turnover* for contraventions of GDPR. The maximum level of the fine varies according to the requirements of GDPR that have been contravened, while the amount of the fine will depend on a number of factors, including whether the contravention was intentional or negligent, any mitigating steps that have been taken, whether the controller or processor complied with a recognised code of conduct or certification scheme, and whether the controller or processor dealt co-operatively with the supervisory authority.

8. **Accountability, impact assessments and privacy by design/default.** Data controllers must be able to *demonstrate* that they comply with the requirements of GDPR, such as through the adoption of privacy policies.

   GDPR requires data controllers to perform impact assessments before carrying out any data processing that is likely to involve high risks for individuals. Where the impact assessment indicates that the processing will involve a high risk, the controller must consult with the supervisory authority before starting the processing.

   GDPR also introduces requirements on 'privacy by design' (requiring data controllers to incorporate measures into their data processing arrangements designed to give effect to the data protection principles) and 'privacy by default' (ensuring that, by default, only personal data that is necessary for each specific purpose of processing is actually processed).

9. **Breach notification.** Data controllers will be required to notify any data breach to the supervisory authority *within 72 hours of discovery*, unless they can show that the breach is unlikely to pose any risk to individuals. High-risk data breaches must also be notified to the individuals themselves, unless the data has been encrypted. Controllers will also be required to maintain a log of all data breaches, whether requiring notification or not.

10. **Requirement to appoint data protection officers (DPOs).** Data controllers and processors will be required to appoint DPOs where their core activities involve regular and systematic monitoring of individuals on a large scale, or involve processing large quantities of sensitive personal data or criminal records. DPOs must be expert in data protection law and practice, and must be allowed to act independently and report directly to top-level management within the organisation.

NEXT STEPS

- **Does GDPR apply to you?** As a first step, assess whether GDPR applies to your organisation (see points 1 and 2). This will be particularly relevant for data processors, and for non-EU data controllers that are not currently subject to EU data protection law.

- **Review legal grounds for data processing.** Data processing that is lawful under current EU data protection law will not automatically continue to be lawful under GDPR. Organisations should review the personal data that they collect (see point 3) and how they process that data, and ensure that all processing has a legal basis under GDPR. Where the legal ground for processing data is consent, this should be assessed against the new requirements in GDPR (see point 4). Particular care should be taken when processing activities include profiling (See point 6).

- **Review fair processing notices.** GDPR sets new standards for information provided to individuals and for obtaining consent. Existing privacy notices, as well as data protection provisions in terms and conditions, should be reviewed for compliance with GDPR.

- **Review contracts.** GDPR contains new requirements for contracts with data processors, as well as contracts between data controllers – and there is no provision that allows existing contracts to continue under GDPR. Third parties should be categorised (as processors or controllers) and contracts reviewed for compliance with GDPR.

- **Review policies and procedures.** Existing privacy and information security policies should be reviewed (or documented, where they do not already exist) for compliance with GDPR, and organisations should ensure that they have processes in place to enable data subjects to exercise their rights under GDPR (see point 5) and to carry out impact assessments where required (see point 8). Organisations providing products and services that collect or process personal data should pay particular attention to the new requirements for privacy by design and privacy by default (see point 8).

- **Do you have to appoint a DPO?** Finally, organisations should determine whether they are required to appoint a DPO (see point 10) and identify suitable candidates (including third party specialists, where appropriate).

DATA PRIVACY AND INFORMATION SECURITY GROUP

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any of the members of our Data Privacy and Information Security Group.

If you would like copies of our other Client Alerts, please visit our website at www.milbank.com and choose "Client Alerts" under "News."