The Law Society

Tim Hickman

Associate, White & Case LLP

Obligations of controllers and processors under the GDPR

Introduction

- Enforcement of the General Data Protection Regulation ("**GDPR**") starts on 25 May 2018.

- Under the GDPR, some things change, but not everything. In general, the GDPR builds on existing principles and adds tighter obligations and restrictions on businesses.

- The concepts of "controller" and "processor" are essentially unchanged under the GDPR, **BUT** their respective obligations are significantly amended.

Key definitions

- "**Controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

- "**Processor**" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

General conditions for processing under Directive 95/46/EC

- **Data quality principles (Art. 6)** – The controller must comply with the "data quality principles" (e.g., the processing of personal data must be fair and lawful; personal data must be adequate, relevant and not excessive; personal data must be accurate and, where necessary, kept up to date; etc.).

- **Legal basis for processing (Art. 7)** – Personal data can only be processed where the controller has a legal basis for that processing (e.g., consent, legitimate interests, contractual necessity, etc.).

Existing key obligations of Controllers under Directive 95/46/EC

- **Appointment of representatives (Art. 4(2))** – Where EU data protection law applies to a Controller established ***outside the EU***, it must appoint a representative in the Member State whose data protection laws apply to it.

- **Appointment of Processors (Art. 17(2)-(3))** – Controllers must appoint a Processor under a ***binding written contract*** which states that the Processor:
  - (i) shall only process personal data in accordance with the Controller's instructions; and
  - (ii) must ensure the security of those personal data.

Existing key obligations of Controllers under Directive 95/46/EC (Cont.)

- **Records of processing activities (Rec. 48; Art. 18)** – Each Controller (and any of its representatives) must notify the relevant Data Protection Authority ("**DPA**") before processing personal data (Member States may simplify this obligation, or provide exemptions – e.g., the appointment of a DPO).

- **Data Security (Rec. 46; Art. 17(1))** – Controllers must implement appropriate technical and organisational security measures to protect personal data.

New key obligations of Controllers under the GDPR

Essentially the similar to the Directive, plus:

- **Data protection "by design" and "by default" (Rec. 78; Art. 25)** – Controllers must ensure that, in the planning phase of processing activities and implementation phase of any new product or service, data protection principles and appropriate safeguards are addressed/ implemented.

- **Joint controllers (Rec. 79; Art. 4(7), 26)** – Where two or more Controllers act together they are "Joint Controllers" and must, by means of an "arrangement" between them, apportion data protection compliance responsibilities.

New key obligations of Controllers under the GDPR (Cont.)

- **Liability of Joint Controllers (Rec. 79, 146; Art. 26(3), 82(3)-(5))** – Joint Controllers are jointly and severally liable. A Joint Controller may be exempt from liability if it proves that it is in no way responsible for the damage. If it pays full compensation to the affected data subjects, then it may bring proceedings against other Joint Controller(s) to recover that compensation.

- **Records of processing activities (Rec. 82, 89; Art. 30)** – There is no obligation to notify DPAs but Controllers must keep records of their processing activities (which include certain prescribed information). Upon request, these records must be disclosed to DPAs.

New key obligations of Controllers under the GDPR (Cont.)

- **Appointment of Processors (Rec. 81; Art.28(1)-(3))** – A Controller must only appoint a Processor under a binding written agreement, which states that the Processor must:
  - (i) only act on the Controller's documented instructions;
  - (ii) impose confidentiality obligations on all personnel who process the relevant data;
  - (iii) ensure the security of the personal data that it processes;
  - (iv) abide by the rules regarding appointment of sub-processors;
  - (v) implement measures to assist the Controller in complying with the rights of data subjects;
  - (vi) assist the Controller is obtaining approval from DPAs where required;
  - (vii) at the Controller's election either return or destroy the personal data at the end of the relationship; and
  - (viii) provide the Controller with all information necessary to demonstrate compliance with the GDPR.

New key obligations of Controllers under the GDPR (Cont.)

- **Reporting data breaches to DPAs (Rec. 73, 85-88; Art. 33)** – Controllers must report a data breach to the relevant DPA within 72 hours of their becoming aware of that breach, except where the data breach is unlikely to result in any harm to data subjects.

- **Notifying data breaches to affected data subjects (Rec. 73, 86-88; Art. 34)** – Where a data breach causes a high degree of risk to data subjects, Controllers must notify the affected data subjects without undue delay. The Controller may be exempt from this in certain situations.

Existing key obligations of Processors under Directive 95/46/EC

- **Appointment as a Processor (Art. 17(2)-(3))** – Controllers must appoint a Processor under a binding written contract which subjects the Processor to the two obligations detailed earlier.

- Under Directive 95/46/EC, Processors owe contractual obligations to the relevant Controller, but have no direct statutory compliance obligations.

…but that's all changing…

New key obligations of Processors under the GDPR

- **Appointment as a Processor (Rec. 81; Art. 28(1)-(3))** – Controllers must appoint a Processor under a binding written contract which subjects the Processor to the eight obligations detailed above.

- **Compliance obligations under the GDPR (Rec. 22; Art. 3(1))** – The GDPR imposes legal compliance obligations directly on Processors (in addition to Controllers).

New key obligations of Processors under the GDPR

- **Failure to comply with the Controller's instructions (Art. 28(10))** – Where a Processor determines the purposes and means of any processing activity, that Processor is treated as a Controller in respect of that processing activity.

- **Records of processing activities (Rec. 82; Art. 30(2))** – Each Processor (and any of its representatives) must keep records of its processing activities performed on behalf of the Controller (which include certain prescribed information).

New key obligations of Processors under the GDPR (Cont.)

- **Cooperation with DPAs (Art. 31)** – Processors (and any of their representatives) are required to cooperate, on request, with DPAs in the performance of their tasks. For many Processors, who are generally not used to dealing with DPAs, this is a potentially significant change.

- **Obligation to appoint a DPO (Art. 37)** – To the extent that the GDPR requires the appointment of a Data Protection Officer (a "**DPO**"), that requirement applies to Processors as well.

New key obligations of Processors under the GDPR (Cont.)

- **Restrictions on Cross-Border Data Transfers (Art. 44)** – The obligation to ensure that there is a lawful basis for all Cross-Border Data Transfers applies directly to Processors as well as controllers.

- **Liability of Processors (Rec. 146; Art. 82(1)-(2))** - Data subjects can bring claims directly against a Processor (but only where it has not complied with its obligations under the GDPR or acted outside/contrary to lawful instructions of the Controller).

Conclusions

- In general, businesses will face increased obligations, whether they act as Controllers or Processors.
- Many Controllers will need to re-negotiate their existing agreements with Processors to bring those agreements into compliance with the GDPR.
- Guidance on how these principles should be interpreted has not yet been published, so it is crucial to keep these issues under review.

The Law Society

Questions?

The Law Society

Thank you.

Tim Hickman
Associate
White & Case
http://www.whitecase.com/eu-gdpr-handbook