Outsourcing contracts under the General Data Protection Regulation: more revolution than evolution

Mr. Olivier Reisch
Counsel
olivier.reisch@linklaters.com

Mr. Maxime d’Angelo
Associate
maxime.dangelo@linklaters.com

The General Data Protection Regulation, which will replace the current Directive 95/46/EC as from 25 May 2018, will profoundly modify the contractual relationship between controllers and service providers acting as processors. The list of obligations that the controller must impose on the processor will be significantly extended, and the regulatory risks associated with non-compliance far greater than before. Now is the right time to adapt outsourcing contracts to the new requirements.

The General Data Protection Regulation (GDPR)1 the long-awaited Regulation which will (i) replace the current Directive 95/46/EC (Data Protection Directive)2 as from 25 May 2018, (ii) reshape the data protection landscape in the EU and (iii) apply directly in all Member States imposes numerous new obligations on both data controllers and processors (such as cloud service providers).

Among other things, article 28 of the GDPR requires that controllers incorporate a long list of clauses in their contracts with service providers acting as processors, covering a wide range of issues.

The purpose of this “new contractual deal” is to ensure the best protection of the individuals whose data are the subject of outsourcing. The compliance risk will weigh on both the data controller and the processor. Combined with increased fines for breach and new powers for supervisory authorities, data subjects’ rights should be better enforced.

From the viewpoints of the data controllers and processors however, it means navigating a sea of legal provisions, redrafting outsourcing contracts and, sometimes, rethinking the business model.

This article explores the main issues that data controllers and processors must address to adapt
their contracts to be in compliance with the GDPR. Compliant contracts and procedures must be in place for 25 May 2018 – and because of the major changes introduced by the GDPR, actions should be taken now.

The current legal requirements

The Data Protection Directive allows organisations that act as controllers to appoint service providers to process personal data on their behalf, under certain conditions.

The controller must appoint the processor in the form of a written contract, under which the processor commits to:

- act only on instructions of the controller;
- ensure the security of the personal data that it processes, by implementing appropriate technical and organisational measures of protection3.

The processor must also ensure that the processed data are kept confidential4.

What changes with the GDPR

Under the GDPR5, the list of contractual obligations that the controller must impose on the processor is significantly extended. The clauses that must be included in the data processing contract may be classified into three categories:

- clauses which impose technical and organisational measures on the processor;
- clauses which increase the communication/cooperation between the controller and the processor;
- clauses which allocate the risk of non-compliance in the performance of the contract between the parties.

1. Clauses which impose technical and organisational measures on the processor

> Sufficient guarantees: the controller can only appoint a processor that provides “sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject”6. This requirement already exists in the Data Protection Directive. In practice, the controller should carefully examine the potential processor before contracting (due-diligence). It should check if the processor participates in a data protection certification or has adopted an approved code of conduct7. The contract should precisely describe the “technical and organisational measures” that the processor has already implemented or will soon implement.

> Records of processing activities: the contract must precisely document the data processing activities (nature, purpose, duration, type of data, categories of data subject)8. Each processor
must keep records of its processing activities performed on behalf of the controller, which represents a significant investment. To that end, the processor could take another look at Luxembourg’s recent law on electronic archiving.

> **Confidentiality**: a confidentiality clause must be stipulated, under which the processor ensures that the persons processing personal data are subject to confidentiality. This clause is standard in data processing contracts.

> **Data security**: the processor must implement measures to ensure a level of security appropriate to the inherent risks to the data being processed.

These measures, which may consist in encryption of data or pseudonymisation, should be listed and described in the contract (as a proof of compliance, to be combined with effective implementation).

> **Deletion of data**: at the end of data processing services and at the discretion of the controller, the processor must delete or return personal data to the controller.

2. **Clauses which increase the communication/cooperation between the controller and the processor**

> **Consent of the controller to subcontracting**: a processor cannot engage another processor without the prior written consent of the controller. Where general consent is attained, “the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes”12. In practice, the contract should stipulate a mechanism allowing the parties to agree upon a solution if the controller objects to the subcontracting.

> **Supply chain control**: the contract must provide that the processor must pass to the sub-processor the same data protection obligations as set out in the contract with the controller. The processor is liable to the controller for the failure of the sub-processor to fulfil its data protection obligations.

> **Instructions from the controller**: the controller must impose an obligation on the processor to act on its instructions, including with regard to transfers of personal data to non-EU countries, unless such data transfers are legally required. The processor must immediately inform the controller if in its opinion an instruction breaches the GDPR or a Member state’s law15. The GDPR now provides that where a processor determines the purposes and means of any processing activity without following the controller’s instructions, that processor is treated as a controller and subject to the obligations of the controller in relation to this processing. The contract should provide for a precise definition of an “instruction from the controller” (e.g. what policies, service levels, technical standards constitute the instructions? does an email containing a specification constitute an instruction? Who is authorised to give an instruction in the controller’s organisation?). It should also provide for a procedure to resolve the issue of the
additional costs incurred by a change of instructions.

> **Requests of the data subjects**: the processor must assist the controller “for the fulfilment of the controller’s obligation to respond to requests for exercising the data subject’s rights”. Data subject rights will be multiplied under the GDPR. The contract should specify the procedure to be followed by the parties in case an individual requests to exercise his/her rights, for every specific right.

> **Breach notification**: the GDPR requires the processor to “notify the controller without undue delay after becoming aware of a personal data breach”17. Under the GDPR, a contractual clause (i) should remind the processor of its obligation and (ii) describe the processor’s data breach detection tools.

> **Availability of information**: the processor must make available to the controller all information necessary to demonstrate compliance with its obligations and allow for audits, either by the controller or an appointed auditor. The “information and audit” clause is essential. The contract should (i) define the information provision obligation, (ii) describe the steps that the parties must follow to conduct the audit, (iii) indicate the level of audit and (iv) specify which party pays for the audit.

3. **Clauses which allocate the risk of non-compliance in the performance of the contract between the parties**

> **Liability and indemnity**: the contract should provide for indemnity caps and exclusions where a GDPR breach occurs and/or the data subjects bring a claim against one or more parties. It should define who bears the risk in the various cases of violation of the obligations set out in the GDPR (especially in the case of a data breach: who pays the incident response costs, the compliance programme implementation costs?).

> **Insurance**: parties should consider, for each risk, whether or not to take out insurance.

**Non-compliance: what is the risk for controllers and processors?**

Controllers and processors failing to comply with article 28 of the GDPR face three sorts of risk:

1. **Fines**
   - Violation of article 28 of the GDPR by the controller or the processor could attract fines of up to 10 million euro or 2% of the global turnover of the previous financial year, whichever is higher18.
   - If the infringement of article 28 also constitutes a breach of other GDPR provisions, it could attract fines of up to 20 million euro or 4% of global turnover of the previous financial year.
   - Fines are likely to be calculated on a group-wide basis19.

LexGO sprl - www.lexgo.lu - (c) 2019 - All rights reserved
2. Claims by individuals

- If both the controller and the processor (i) are involved in the same processing and (ii) are responsible for any damage caused by this processing, they shall be jointly liable for compensation claims by individuals. Individuals will have the right to recover both material damage and non-material damage (e.g. distress).

3. Other sanctions

- Supervisory authorities may enforce an individual’s rights, issue a warning or issue a temporary or permanent ban on processing;
- Under current Luxembourg law, a violation of data protection obligations is subject to criminal sanctions. It is as yet uncertain whether these sanctions will be maintained after the coming into force of the GDPR.

Controllers and processors thus have a lot to gain by regularly informing each and cooperating in order to ensure that they both comply with the provisions of the GDPR.

What to do now?

- **For both the controller and the processor**: (i) reviewing the existing data processing contracts, (ii) assessing whether amendment is needed or not, (iii) regularly checking for further guidance from EU and national authorities.
- **For the controller only**: assessing the ability of current contracting processors to comply with the GDPR. If it is not the case, contracts with these parties should not be renewed. When assessing the value of a processing service, controllers cannot solely consider the cost anymore. They must also consider the capacity of the service to perform the contract in accordance with the GDPR. This capacity can be demonstrated by the participation of the processor in a certification programme approved by supervisory authorities or the adoption by the processor of a code of conduct.
- **For the processor**: (i) analysing its new obligations under the GDPR, (ii) verifying that procedures to identify, assess and promptly report data breaches to the controller are in place, (iii) reviewing the existing sub-processing contracts, (iv) assessing whether participating in a data protection certification or adopting an approved code of conduct is necessary or not.

---

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of
personal data and on the free movement of such data.
3 Data Protection Directive, article 17, paragraph 3.
4 Data Protection Directive, article 16.
5 GDPR, article 28, paragraphs 1 and 3.
6 GDPR, article 28, paragraph 1.
7 GDPR, article 28, paragraph 5: “adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article”.
8 GDPR, article 28, paragraph 3.
9 GDPR, article 30, paragraph 2.
11 GDPR, article 28, paragraph 3. (c).
12 GDPR, article 28, paragraph 2.
13 GDPR, article 28, paragraph 4.
14 GDPR, article 29.
15 GDPR, article 8, paragraph 3.
16 GDPR, article 28, paragraph 10.
17 GDPR, article 33, paragraphs 2 and 3.
18 GDPR, article 83, paragraph 4.
19 Administrative fines are applied to “undertakings”, defined by reference to articles 101 and 10 of the Treaty on the Functioning of the European Union. Undertakings, as economic units, could potentially include the companies of a same group.
20 GDPR, article 82, paragraph 3.
21 GDPR, article 58, paragraph 2.