astura
AVOCATS À LA COUR

# GDPR: STRENGTHENING OF DATA PROCESSOR'S OBLIGATIONS - PRACTICAL GUIDANCE FROM THE CNIL

*The General Data Protection Regulation n°2016/679 (the "**GDPR**"), which will enter into force on May 25th, 2018 in all EU countries, implements new obligations on every legal entity or natural person processing personal data outside the course of a purely personal or household activity.*

*While the current regime only imposes obligations on the data controller, the GDPR also draws out obligations directly towards the data processor.*

*Any service provider which processes personal data for its customers must therefore comply with a set of obligations in accordance with the GDPR.*

*The French data protection authority (the "**CNIL**") published a practical guide on September 29th 2017 where it specifies what is a data processor and details the obligations and measures that it should be taking. Here is a summary of the key points to keep in mind in order to ensure compliance of data processors with their new obligations.*

## 1. WHO IS CONCERNED?

The GDPR follows the current data protection regulation according to which a data processor is the entity which processes personal data on behalf of and under the instruction of the data controller (i.e., its client). The CNIL gives some practical examples, including:

- maintenance and hosting service providers;
- software integrators;
- cyber security companies;
- computer services and engineering companies;
- marketing or communication agencies processing personal data on behalf of their customers.

## 2. TEMPLATE OF DATA PROCESSING CLAUSES TO BE INSERTED IN CONTRACTS BETWEEN DATA CONTROLLERS AND DATA PROCESSORS

The GDPR imposes new clauses that must be included in all contracts between data controllers and data processors.

These clauses should be incorporated into your contract policy for the future contracts and existing contracts should be amended so as to comply with the GDPR as of May 25th, 2018.

To ease the process, the CNIL has set out a fairly complete template in its practical guide and the WP29 (a group composed of all the European data protection authorities) is to adopt standard contractual clauses.

### 3. MAINTAIN A RECORD OF DATA PROCESSING ACTIVITIES

Each data processor shall maintain a record of all personal data processing carried out on behalf of its customers (categories of data processed, contact details of the customers, potential transfers of personal data to a country outside of the EU).

As a reminder, the service provider will also act as a data controller when processing personal data for its proper activities (such as HR, management of its own customers database, etc.)

The service provider will therefore have to keep two separate registers: one for the personal data processed as data controller, the other one for the personal data processed on behalf of its customers, as data processor.

### 4. APPOINT A DATA PROTECTION OFFICER (« DPO »)

The GDPR requires both data controllers and data processors to appoint a DPO. This obligation is applicable to companies whose main activities require (i) regular and systematic monitoring of data subjects on a large-scale (such as the monitoring of an e-commerce website or the management of customers databases), or (ii) to process special categories of personal data called sensitive data (such as health data) on a large-scale.

The WP29 suggests, in its guidelines adopted on April 5th, 2017, that the DPO designated by the data processor should be responsible not only for controlling the service provider's activities when processing data as data processor, but also when processing data on its own behalf as, data controller (HR, management of its own customers database, etc.)

In any event, the CNIL recommends to appoint a DPO even if the data processor is not under the obligation to do so in order to have an expert dedicated to the protection of personal data and to supervise compliance with the GDPR.

### 5. ASSIST ITS CUSTOMER IN IMPLEMENTING PROCESSING

The CNIL specifies the role of the data processor in assisting its customers with their obligations of information and of assistance. The data processor will thus have to:

- assist the customer to enable the data subject to exercise their rights (such as access, rectification, erasure, portability, the right to object, the right not to be subject to an individual decision);

- assist the customer in carrying out a data protection impact assessment (the "**PIA**"), although the PIA in itself is the responsibility of the customer;

- alert the customer if, in its opinion, a customer instruction infringes personal data protection rules. In this regard, we recommend that this obligation be limited to an obligation of information without being extended to an obligation to advise, as the data processor is not a legal adviser.

### 6. ALERT ITS CUSTOMER IN CASE OF A SECURITY BREACH

The data processor must notify its customer of any personal data breach as soon as possible after becoming aware of it.

The customer shall then, if necessary, notify the competent authority and communicate the personal data breach to the data subject. In this regard, the CNIL indicates that the customer may also ask the data processor to make this notification and communication on its behalf. From a legal stand point, this task could be framed by drafting a mandate, under which the data processor represents the customer in its name and on its behalf.

### 7. OBTAIN CUSTOMER'S AGREEMENT IN CASE OF SUB-PROCESSING

The data processor must obtain its customer's agreement when subcontracting its obligations. This authorization may be granted to a specific sub-processor or generally granted. In this case, the data processor must inform the customer of any change of sub-processor and the customer may object such change. Note that, in any event, the customer's consent will be necessary in order to comply with French law on subcontracting dated 31 December 1975.

The CNIL recalls that the data processor remains fully liable towards the customer for the performance of sub-processors' obligations.

### 8. TAKE INTO ACCOUNT THE *PRIVACY BY DESIGN* AND *PRIVACY BY DEFAULT*

The data processor must provide tools that enable the customer to observe the principle of privacy by design and privacy by default. The CNIL gives practical examples of the functionalities that should be part of these tools, which include:

- allowing the customer to configure by default and minimize the collection of personal data;
- collecting only the data strictly necessary for the purpose of the processing;
- automatically and selectively purging data from an active database after a certain duration;
- managing computer data access rights and privileges.

### 9. RISK OF NON-COMPLIANCE BY A DATA PROCESSOR

Non-compliance with the GDPR can amount to 10 to 20 million euros or up to 2% or 4% of a company's worldwide annual turnover and gives examples that could apply to data processors, including:

- the fact for the data processor to act outside of the scope of or in contradiction with the instructions of the data controller;
- failure to inform the data controller that an instruction would infringe the GDPR;
- the fact for the data processor to sub-process without the data controller's authorization;
- failure to keep a record of data processing activities.

## ABOUT ASTURA

Astura is a boutique law firm specialized in advising businesses and their managers. Astura advises companies and investors in connection with the growth of their businesses on a domestic and international level.

In particular, Astura has been recommended by the Legal 500:

- **information technology***: Astura is 'one of the best price/performance ratio' on the market in terms of expertise and service. The lawyers have 'an excellent knowledge of information technology' and advise several large French and foreign companies in the negotiations of important IT agreements, as well as in conducting litigation and in personal data issues. Matthieu Mélin is amongst 'the best specialists' on the market.*

- **mergers and acquisitions:** *Astura offers 'an outstanding quality of services', the firm is recognized for 'the valuable international experience of its lawyers, their reactivity and their capacity to deliver tailored advice', the team 'is used to working for international sponsors and understands the fundamentals of a deal and the expectations of all types of clients', heading the team, Raphaël Dalmas is 'extremely reactive, adaptable and perfectly comprehends the expectations of his clients';*

## CONTACTS


| Matthieu Mélin | Raphaël Dalmas | Clotilde Chabre |
|---|---|---|
| mmelin@astura.fr | rdalmas@astura.fr | cchabre@astura.fr |
| T +33 (0)1 84 16 24 31 | T +33 (0)1 84 16 24 32 | T +33 (0)1 84 16 24 36 |

www.astura.fr