58, avenue Kléber - 75116 Paris T. +33 1 53 53 44 44 F. +33 1 53 96 04 20
Toque K30 . SELARL au capital de 480 000 euros . RCS Paris B 393 584 347

Representations and Warranties and Compliance with the General Data Protection Regulation – Application of the GDPR by 25 May 2018

Laurent Marville, partner

In the big data era, the massification of information has become a priority for businesses. The issue of the legal rules applicable to the use of personal data for economic purposes is thus one of key importance.

France, a pioneer in the establishment of regulations creating and protecting the rights of individuals in respect of the use of their personal data (since the adoption of France's data protection act of 6 January 1978), has been a model for a large number of countries worldwide. Now, the European Union, conscious of both the growing economic importance of data as an asset in its own right and of the disparities in systems of protection of individual data subjects even between its own Member States, has become the torch bearer on the issue of defending personal data privacy and establishing a harmonized set of rules for the whole European Union.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 94/46/EC (hereinafter the "General Data Protection Regulation" or the "GDPR") of 27 April 2016 is the result of a compromise between the traditional French conception of a system founded on the protection of personal rights and the Anglo-Saxon model which takes account of economic necessities and the need to allow the use of personal data as the digital economy innovates and expands.

The GDPR:

- creates a unified legal framework for the whole European Union, which will allow the free flow of personal data within the single market, and
- maintains the possibility of transfer of personal data to third countries where such countries have been the subject of an adequacy decision of the European Commission, finding that such country ensures an adequate level of protection of data subjects which is compatible with the GDPR's requirements, but provides that such adequacy decisions must be subject to periodic review. The GDPR also recognizes the possibility to transfer personal data outside the European Union using approved contractual clauses, binding corporate rules, codes of conduct or on the basis of a new certification mechanism. We can expect, however, that the compatibility of these grounds of transfer with EU Charter of Fundamental Rights will be the subject of references to the

European Court of Justice in the future (as have been the case with the grounds of transfer authorized in Directive 94/46/EC).

Any economic operator established within the European Union or any economic operator that collects and processes the personal data of persons resident in the European Union must put in place, by 25 May 2018, suitable measures of protection of personal data guaranteeing an appropriate level of protection of the rights of data subjects and the security of the data.

The GDPR thus represents a shift from a system of rules based on *ex ante* control by data protection authorities to a system of accountability of the economic operators that handle personal data.

Personal data consists of information that allows a natural person to be identified directly, indirectly or by the cross-referencing of data that does not of itself identify the natural person (referred to in the GDPR as the "data subject"). Within this category of personal data, we can distinguish so-called "sensitive" data, i.e. those concerning the data subject's state of health (and more generally, any aspect relating to physical or physiological characteristics), which is subject to special protection and whose use is possible but more restricted.

Data subjects whose data is collected by an economic operator, for any reason whatsoever, must expressly consent to the processing of their personal data and must be able to exercise, at any time, a certain number of rights in relation to such data, in particular a right of access, a right to be forgotten, a right to restriction of processing and a right to data portability.

The effectiveness of the exercise of such rights of data subjects is a critical component of the GDPR and the economic operators are themselves responsible for ensuring such rights are effective, thus leading many of them to reconsider the nature of the relationship with their customers.

Indeed, this constraint of the GDPR and the obligation to confer effective rights on data subjects, that can be easily accessed and exercised, has constituted an opportunity for economic operators to renew their relationships with customers.

The GDPR thus explicitly integrates a principle of "Accountability" of economic operators.

In order to ensure compliance with these regulations, whereby economic operators are themselves the guarantors of effective data protection, the GDPR significantly increases the sanctions that may apply in case of breach of its provisions.

Thus, the sanctions that may be imposed by the data protection authority, or "supervisory authority" to use the GDPR terminology, (namely the CNIL in France), may go up to 20 million euros or 4% of worldwide turnover, whichever is higher.

The GDPR is therefore deliberately intended to effectively incite economic operators to take measures to comply with the regulations as quickly as possible.

The scope of such sanctions is also intended to counteract major economic players in the worldwide economy who process data and, coming from countries that do not have strong

legal protection of privacy and personal data in place, for whom respect for data privacy has not been a matter of high priority.

Based on the regulations, any M&A transaction must firstly involve an assessment of the business of the target company in order to determine its level of exposure to data protection obligations. This means first mapping all of the data processing activities carried out by the target to determine the exact nature of its functions, namely either:

- those of a controller (defined in Article 1 of the GDPR as the person or entity "*which, alone or jointly with others, determines the purposes and means of processing of personal data*") ; or
- those of a processor (defined in Article 1 of the GDPR as the person or entity "*which processes personal data on behalf of the controller*").

This analysis is sometimes subtle and complex but is however essential as it will have an impact in terms of the resulting representations and warranties required in the transaction.

For example, it is essential to bear in mind that the controller is not only required to include clauses in its contracts with its processors imposing strict requirements in relation to the security of data entrusted to the processors, but must also monitor and supervise sensitive data processing operations carried out by the processors.

In a decision of 19 July 2017, the French data protection authority CNIL sanctioned the company Hertz in respect of a data security breach of one of its processors, on the basis that Hertz should have ensured that the processor had conducted tests to verify that its system was not vulnerable in any way. This decision emphasizes the obligation of the controller to remain in continuous contact with its processors and to supervise any sensitive data processing operations they carry out.

The position adopted by the CNIL is consistent with the judgment of the French Council of State of 11 March 2015 which held that, even if the contract places obligations of security on the processor, this contractual requirement does not release the controller from its responsibility to ensure the security of the data and to monitor the processor's compliance with its contractual undertakings in reality.

The representations and warranties should include undertakings on this issue and provide confirmation that inspections and audits have been carried out at the processors' sites.

Mere declarations of the seller are not sufficient and it is important to use the opportunity of the due diligence review prior to the transaction to review the nature of the target's operations in order to verify the scope of the required representations and warranties and the target's effective compliance with data privacy legislation.

Similarly, a prior analysis of the target's involvement in processing of personal data and the measures at its disposal to ensure compliance will allow the obligations incumbent on it to be identified and in particular, if the target:

(i) needs to maintain a record of processing activities (Article 30 of the GDPR) containing the name and contact details of the controllers, the purposes of the processing, a description of the categories of data subjects and of the categories of personal data.
This requirement applies to both controllers and to processors, who must maintain a record of all processing activities carried out on behalf of a controller. It does not apply however to companies or organizations with less than 250 employees unless the processing it carries out is "*likely to result in a risk to the rights and freedoms of data subjects*".

However, it is strongly recommended to other large companies (even below the threshold) to keep a record on behalf of the controller. This will be the primary element that can be relied upon vis-à-vis a data protection authority in case of an audit or inspection.

(ii) is required to designate a data protection officer ("DPO") due to the scope or nature of its data processing activities. The role of the DPO, as stated in Article 39 of the GDPR, is to "*inform and advise*" the controller on its obligations pursuant to the GDPR. The DPO should also "*monitor*" compliance with the GDPR and data protection provisions, including the assignment of responsibilities and the training of staff.
At the same time, the DPO is also required to "*cooperate with the supervisory authority*." The DPO's role and position in the company, as the guarantor of compliance with the regulations, who is only answerable to the controller (or the processor, as the case may be) and cannot be assigned any other tasks and duties that would result in a conflict of interest, means that he or she occupies a unique position in the company.

(iii) must conduct a data protection impact assessment prior to any type of processing likely to result in a high risk to the rights and freedoms of natural persons (Article 35 GDPR).

This impact assessment must:
- specify the measures, safeguards and mechanisms intended to reduce the potential risk to the rights and freedoms of data subjects;
- ensure the protection of personal data; and
- demonstrate that the data processing is compliant with the GDPR.

If such impact assessment reveals a high risk for the rights and freedoms of data subjects, which cannot be mitigated by taking appropriate measures, the supervisory authority, i.e. the CNIL in case of France, must firstly be consulted prior to such processing (Article 36 GDPR).

(iv) document any personal data breaches in order to comply with the GDPR's requirements on this subject.

Indeed, in the event of a personal data breach, the economic operator, as controller, is obliged to notify the CNIL of such data breach within a maximum period of 72 hours after becoming aware of it (Article 33 of the GDPR) and inform the data subject(s) concerned of the personal data breach where it is likely to result in a high risk to the rights and freedoms of the data subject(s) (Article 34 of the GDPR).

The processor is not subject to these obligations but is required to inform the controller of the personal data breach without undue delay (Article 33 of the GDPR).

In conclusion, it is important to bear in mind that the issue of GDPR compliance needs to be henceforth systematically integrated into the process of acquisition of a business that processes personal data, having regard to the active role that the GDPR confers on economic operators in ensuring their own compliance as well as the scope of the responsibilities in play.

Such vigilance is especially important in the current transitional period when companies must shift from a model where compliance was essentially based on the making of declarations (easy to verify), towards a new approach where compliance is a collective challenge for the entire company.

In practice, a M&A lawyer should at least take the following precautions to address data protection compliance:

(i) At the due diligence phase

The purchaser should obtain all necessary proof of the target's GDPR compliance, in particular:

- The record of data processing (this record will in particular allow verification that all of the target's processing activities were for lawful purposes);
- Any impact assessments carried out;
- The record of personal data breaches;
- Consent forms;
- Contracts relating to data processing and partnerships involving an exchange of personal data;
- Proof that the IT programs used by the target are GDPR compliant (human resources and payroll software, monitoring equipment and geolocation equipment);
- The IT charter;
- The personal data and privacy policy;
- All correspondence with the CNIL relating to the application of the GDPR, or any audit report of the CNIL;
- The contract, the description of tasks and the place in the company's organization chart of any data protection officer.

The purchaser should pay particular attention to the content of the audit report concerning the level of compliance of the data protection system established by the target.

More specifically, the purchaser should also ensure that the purposes of the data processing conducted by the target are consistent with its corporate objects.

(ii) In the drafting of representations and warranties

Concerning the seller's representations and warranties, the purchaser cannot simply accept a general declaration of the target's compliance with the GDPR, given that the company is required to have a multifaceted system in place to ensure compliance.

In particular, depending on the role of the target in the processing of data (controller or processor) and the extent of the processing, due to either the volume of data or its nature (such as sensitive data), the purchaser should insist on certain aspects of compliance, including:

- Due respect for the rights of data subjects and the effective possibility for such data subjects to exercise those rights;
- The use of IT tools ensuring real protection of data and secure access by data subjects, meaning that the seller should give representations about the audits and inspections carried out, both in relation to the target's own data security systems and those of its processors (if the target is the controller);
- The implementation of contractual risk mapping with all processors to limit the liability of the controller;
- The use of the compliance tools provided in the GDPR.