English translation for information purposes of an article
published in Revue Lamy Droit des affaires No. 145, February 2019

Tribune

RLDA 6655 (Nº 145 February 2019)

The new personal data protection rules in merger & acquisition transactions

Charles Dauthier
Partner
Morgan Lewis

Laetitia de Pelet
Associate
Morgan Lewis

This article addresses the ways to ensure compliance of a merger & acquisition transaction, and the preliminary audit thereof, with applicable personal data protection regulations[1].

Introduction

For several months, the legal community has been working towards compliance with Regulation (EU) 2016/679 on the protection of personal data (GDPR)[2] and the amended version of act no. 78-17 (on information technology, data files and civil liberties, "*Loi Informatique et Libertés*".)[3].

The application of this new legislation has a strong impact on the business community, merger & acquisition transactions being no exception to the rule.

Today, personal data protection must be a necessary focus of attention in the context of such transactions, both in terms of respecting the rights of the people whose data is processed, and in terms or safeguarding their value, which currently represents a substantial portion of the valuation of many economic operators. Indeed today, intangible assets represent nearly 84 % of the total value of Fortune 500 companies[4]. These intangible assets include, *inter alia*, client and HR files.

The transfer of ownership of such files requires special attention in the case of M&A transactions, both at the time of the preliminary legal audit and at the time of formalizing and documenting the relevant transaction.

This study aims to provide a few elements of analysis on these issues, considering the recent reforms.

---

[1] It is not intended to be a guide on how to conduct a data privacy audit, or an exhaustive list of the items to be checked during such audit.
[2] Reg. (EU) 2016/679, 27 Apr. 2016, 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 95/46/EC, entered into force on 25 May 2018.
[3] Act no. 78-17, 6 Jan. 1978, on information technology, data files and civil liberties, amended by act no. 2018-493 of 20 June 2018 on personal data protection.
[4] *Opérations de M&A et protection des données personnelles : identifier et minimiser les risques*, H. Segain and J.-B. Thomas-Sertillanges, Fusions & Acquisitions.

I. – Legal audit and GDPR

A. – Self-monitoring system implemented by the GDPR

Until 25 May 2018, the vast majority of personal data processing required taking preliminary steps with the French National commission on information technology and liberties (*Commission nationale de l'Informatique et des Libertés*) (CNIL).

The procedure to be followed varied in particular according to the type of data processed and the risks associated with the relevant processing. It could prove quite simple (simplified declaration, or standard declaration) or more complex (request for authorization) in some cases.

One of the great contributions of the GDPR and of the *Loi Informatique et Libertés* results from the abolition of such formalities in a large majority of cases.

The approach adopted is now different: the role of the prior check is reduced and self-monitoring is currently favored.

This self-monitoring requires observing three main principles established by the new regulation:

— Accountability: the obligation for companies to implement internal mechanisms and procedures which allow demonstrating compliance with personal data protection rules[5];

— Privacy by Default: the obligation to ensure that, "by default", only personal data which is necessary for each specific purpose of the processing is processed[6];

— Privacy by Design: the obligation to take account of the personal data protection requirement as soon upon designing projects, products or procedures.[7]

The assertion that these principles are observed will obviously not be sufficient in case of control: the observance of such principles needs to be constantly documented.

Given the rather abstract nature of the three aforementioned principles, this documentation may prove difficult to implement in practice.

B. – Practical implementation

The GDPR and the *Loi Informatique et Libertés* apply "[…] *to the automatic processing in whole or in part of personal data as well as to the non-automatic processing of personal data that is are or may be contained in a filing system* […]"[8].

[5] CNIL glossary consulted on 18 December 2018.
[6] Reg. (EU) 2016/679, art. 25.2.
[7] Reg. (EU) 2016/679, art. 24.1.
[8] Act no. 78-17, art. 2.

As such, the easy option is to avoid applying the personal data protection regulations by anonymizing all of the documents provided as part of the legal audit, subject to the data that would already have been published (for instance information contained in K-bis, such as the name of the corporate representative or his/her personal address)[9].

However, this solution may prove quite tedious to implement if several documents are to be provided, insofar as the legal definition of personal data is very broad.

Besides, this process is difficult to automate since some data may in some instances be personal and not in other[10].

Hence, anonymization only seems suitable in the case of very small audit operations.

Failing anonymization, the GDPR and the *Loi Informatique et Libertés* shall be fully applicable.

Under this scenario, in accordance with the aforementioned privacy by design principle, it may be appropriate[11] to assess the risk that the personal data processing used as a result of the legal audit would entail. In principle, this risk assessment should take the form of an "*assessment of the impact of the contemplated processing operations on the protection of personal data*."[12] For that matter, the CNIL has released a new so-called "PIA" free software in order to help companies formalize and conduct these impact assessments in compliance with GDPR and with the *Loi Informatique et Libertés*[13].

Carrying out such an assessment also ensures compliance with the accountability principle by allowing documenting the compliance of the analyzed processing.

However, implementing such an assessment may prove extremely cumbersome and ill-adapted to the practical reality of an audit considering, in particular, confidentiality and the very tight timetable often imposed by the relevant transaction.

To ensure compliance of the audit with the applicable data protection regulations, one should, at the minimum, previously inform any person whose data will be processed during such audit. This information allows observing the privacy by design principle and the accountability principle, provided that it is made in writing with a proof of delivery (sent by email with request for acknowledgement of receipt and read receipt, delivered against receipt, etc.). It is advised – or at least strongly recommended – to anticipate such information and provide for such audit and restructuring operations within the data protection charter(s) applicable to the company.

---

[9] However, it is important to make a distinction between "*anonymization"* and "*pseudonymization*". It will not be sufficient, to avoid applying the *Loi Informatique et Libertés*, to merely replace the personal data with an identification key. As for the data anonymization technique, it destroys any possibility for anyone to be able to identify to which individual the personal data belongs.

[10] As an illustration, an employee's classification could become a personal data allowing his or her identification, where such employee would be the only one classified as such.

[11] The conduct of an audit is not included in the list of types of processing activities for which a data protection impact assessment is expressly required (CNIL deliberation No. 2018-327, 11 Oct. 2018). However, this activity can potentially meet certain criteria established by G29 in its WP 248 guidelines adopted on 4 April 2017. Compliance with the rules applicable to protection of the data of the implemented audit must, in any event, be documented.

[12] Reg. (EU) 2016/679, art. 35 1.

[13] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

In particular, the information should relate to the personal data in question, the recipients or the intended purpose thereof.

There would be no point in trying to circumvent the constraint deriving from the application of the legal provisions on personal data protection by providing access to a data room only to those lawyers bound by an obligation of professional secrecy. Indeed, the scope of such rules does not provide for any exception in respect of this specific case.

Therefore, the GDPR and the *Loi Informatique et Libertés* have some bearing on legal audit operations. Companies should be aware thereof and adapt their practice. The GDPR and the *Loi Informatique et Libertés* must also be taken into account when formalizing the documents of the relavant merger & acquisition transaction.

II. – The data privacy risk in certain merger & acquisition transactions

Personal data processing is defined as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*"[14].

Given this very broad definition, an activity or a business transfer and the preparation thereof necessarily require processing some personal data (that of employees, clients and other parties involved) and is hence subject to the GDPR and the *Loi Informatique et Libertés*.

Yet, in addition to financial sanctions, the risks incurred in case of breach of this rule are material. Indeed, the contemplated transfer could simply be cancelled. Arrangements should thus be implemented that ensure compliance of the operation with the GDPR and the *Loi Informatique et Libertés*. In any event, the transferee will need to take different steps and perform different checks.

A. – Cancellation of the transfer for non-compliance with applicable personal data protection regulations

The Court of cassation found that a transfer of files could be cancelled for non-compliance with applicable personal data protection regulations[15].

In this case, a computerized client file had not been declared to the CNIL whereas it should have been under the previous regulations. The company holding such file transferred it to a third party. An action was subsequently brought against it for cancellation of the sale. The trial court merely stated that the law does not provide that the lack of such declaration to the CNIL entails cancellation. However, the Court of cassation considered that, since it had not been declared, the client file was not available on the market and that as a consequence, its sale had an unlawful purpose. The high magistrates hence found that the trial court had wrongfully refused to declare the cancellation of the sale for unlawful purpose.

[14] Reg. (UE) 2016/679, art. 4.
[15] Cass. soc., 25 June 2013, No. 12-17.037, JCP E 2013, 1422, note J.-B. Seube; D. 2013. 1867, note Beaussonie; *ibid.* 1844, point de vue Storrer; RTD civ. 2013. 595, obs. Barbier; JCP 2013, No. 930, note Debet; RDC 2013. 119, note Rochfeld.

Although a vast majority of the obligations of prior declaration to the CNIL no longer exist since 25 May 2018, we believe that this approach can be extended to other situations to punish a breach of any of their obligations by the data controllers. This extension is all the more practicable since (i) the CNIL's increased powers relating to supervision and the imposition of penalties could raise concerns of civil courts being more stringent with respect to data protection and (ii) the GDPR increased data controllers' obligations with the intent to make them more accountable.

In that respect, an authorized doctrine recently indicated that "*the entry into an agreement for the sale of personal data collected, processed or transferred unlawfully shall continue to entail cancellation. This would be the case if the personal data was processed without any basis*.[16]" In our view, the same could apply in case of failure by the transferor to comply with its prior notification obligation[17].

It is therefore essential, to secure the validity of the transfer, to check compliance of the transferred files with applicable personal data protection regulations (potential declarations or requests for prior authorization with the CNIL, conduct of impact assessments, information concerning the relevant persons, obtaining the necessary consents, etc.), failing which the operation might be cancelled.

B. – How can the risks of cancellation of the transfer be mitigated?

It is essential to verify compliance of the files transferred as part of the operation with applicable personal data protection rules in order to mitigate the risk of the transfer being cancelled. This requires the implementation of different practices.

First of all, one should of course carry out a data privacy audit of the target of the merger & acquisition transaction. It is nowadays impossible to set this step aside in this type of transactions, all the more since, in addition to the potential cancellation of the transfer agreement, there is now a well-known risk to be sentenced to pay significant administrative fines in an amount that can reach 20 million euros or equal 4% of the aggregate global annual turnover of the previous fiscal year.

Moreover, in case an irregularity is established, if the relevant transaction is an asset transfer and involves the transfer of one or more files, such as a client file, it is advised to subject the transfer to the satisfaction of one or more conditions precedent requiring the seller to regularize the situation and to bring the said file into compliance with applicable personal data protection regulations prior to the transfer of ownership.

Finally, after completion of the transaction, in case the data controller changes, the new data controller should enter into contact with the persons whose personal data is processed in order to observe the notification obligation to which it is bound. This is notably the case with respect to business transfers.

The significance of the changes brought about by the new personal data protection rules is such that an approach whereby resources should be mobilized in order to be GDPR-compliant at a given time would be pointless. Many operators still think that the data protection theme is a passing trend and only aspire to get rid of the matter. This reveals a failure to understand the paradigm shift in the new regulatory framework. Beyond the technical and legal investments which are required to be made in order to bring an organization's

[16] J.-M. Bruguières, V. Fauchoux and A. Quiquerez, Actualité *du droit civil du numérique*, RLDC 2018/162, n° 6477.
[17] Regarding this notification information, see above, I, B).

procedures in line with the GDPR, a vast educational work must be undertaken to raise its coworkers' awareness. Those involved in M&A transactions cannot escape this fact.