LES ENTREPRISES AU REGARD DU REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES : QUELLES REFORMES A OPERER ?

COMPANIES AND GENERAL DATA PROTECTION REGULATION: WHAT REFORMS ARE NEEDED?

Clotilde CAMUS,* David CHEKROUN** et Patrick-Hubert PETIT***

LT Data processing; Data protection; Data protection officers; EU law; Implementation; Privacy by design

Cet article est issu d'une série de conférences organisées et d'entretiens réalisés sur le Règlement Général sur la Protection des Données. Ces conférences et entretiens ont mis en lumière une certaine appréhension des entreprises quant aux implications pratiques du Règlement. Les statistiques révèlent d'ailleurs le retard d'un grand nombre d'entreprises dans leur mise en conformité au Règlement.

L'objectif de cet article est donc de présenter de manière concrète les principales réformes que les entreprises doivent mettre en œuvre afin d'être en conformité avec les obligations posées par le Règlement. A cette fin, l'article se propose de capitaliser sur l'expérience pratique d'opérationnels qui traitent de ces problématiques au sein de leurs entreprises, ainsi que de la littérature existante sur le sujet.

This article is the result of a series of conferences and interviews on the EU General Data Protection Regulation. These conferences and interviews highlighted companies' apprehension regarding the practical implications of the Regulation. The statistics also show that many of these companies are experiencing delays in ensuring compliance with the Regulation.

The article aims at providing a concrete overview of the main reforms that companies have to implement in order to comply with the obligations set forth in the Regulation. To this end, the article seeks to capitalise on the practical experience of operational staff who deal with these issues within their companies, as well as on the existing literature on the subject.

Les auteurs tiennent à exprimer toute leur gratitude et à remercier très chaleureusement pour leur contribution notamment Vincent Maret,[1] Édouard Mercier,[2] Romain Perray,[3] Samuel Profumo,[4] Olivier Rigaudy[5] et Lucy Savary,[6] qui ont accepté de répondre à nos questions tout

The authors would like to extend their sincerest gratitude to all those who have contributed to this article, particularly Vincent Maret, Edward Mercier, Romain Perray, Samuel Profumo, Olivier Rigaudy and Lucy Savary, who agreed to answer our questions and offer their expertise. The views and comments expressed in

* Docteur en droit et chargée de mission au sein du KMPG Professorship in International Corporate Governance.
** Professeur de droit des affaires internationales à ESCP Europe, Directeur scientifique du KPMG Professorship in International Corporate Governance et Visiting Associate Professor of Law, Division of Social Science, New York University Abu Dhabi.
*** Associé KPMG SA, Président de l'Audit Committee Institute France et Président du Comité d'orientation du KPMG Professorship in International Corporate Governance à ESCP Europe.

this article are those of the authors and are not exhaustive.

en apportant leur expertise. Bien entendu, les points de vue et commentaires exprimés dans cet article n'engagent que ses auteurs et ne sauraient prétendre à exhaustivité.

The objective of this article is to present and discuss in practical terms the main reforms that companies must implement in order to comply with the obligations set forth in the General Data Protection Regulation.

Cet article a pour objectif de présenter et commenter de manière concrète les principales réformes que les entreprises doivent mettre en œuvre afin d'être en conformité avec les obligations posées par le Règlement général sur la protection des données.

The major change introduced by the Regulation is the transition from a system involving a declaration to the CNIL (French National Data Protection Commission) to one that requires the company itself to perform day-to-day monitoring activities. In exchange for this freedom (the current scheme is no longer based on reporting requirements), the European legislation imposes an accountability principle on companies. Under this principle, companies must on the one hand be able to take technical, organisational and legal measures on their own to comply with personal data law, and on the other hand be able to demonstrate their compliance at any given time (including through detailed documentation).

Le changement majeur apporté par le Règlement réside dans le passage d'une logique déclarative effectuée auprès de la CNIL à un contrôle au jour le jour fait par l'entreprise elle-même. En échange de cette liberté (le dispositif actuel ne repose plus sur un système d'obligations déclaratives), le législateur européen impose un principe d'*accountability*, de responsabilisation des entreprises. En vertu de ce principe, les entreprises devront, d'une part, être capables de prendre elles-mêmes des mesures — techniques, organisationnelles et juridiques — pour se conformer au droit des données personnelles, et d'autre part, être en mesure de démontrer leur conformité à tout moment (notamment à travers une documentation détaillée).

Although the Regulation sets only a general framework, without determining the specific means of implementing this principle, three main focuses of the reform can be identified:

Si le Règlement se borne à fixer un cadre général, sans déterminer les moyens concrets de mise en œuvre de ce principe, trois principaux axes de réforme peuvent se dégager :

- the compulsory appointment of a data protection officer for companies whose core business includes the regular and systematic large-scale monitoring of people or the large-scale processing of what is considered ''sensitive'' data, or data related to criminal convictions and offences;

- la désignation obligatoire d'un délégué à la protection des données pour les entreprises dont l'activité de base consiste à réaliser un suivi régulier et systématique des personnes à grande échelle ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et à des infractions ;

- the obligation to protect data as early as the design stage of the data processing system (Privacy by Design) and to do so by default (Privacy by Default). Therefore, data controllers and sub-processors must on the one hand ensure that a product, service, application or solution complies with the Regulation throughout its entire life cycle; and on the other hand, by default, collect and process only the personal data that is strictly necessary for the purpose for which the processing of data is intended;

- l'obligation de protéger les données dès la conception des traitements des données (*Privacy By Design*) et par défaut (*Privacy By Default*). Ainsi, les responsables de traitements et sous-traitants devront, d'une part, dès le stade de développement ainsi que tout au long du cycle de vie d'un produit, d'un service, d'une application ou d'une solution, assurer sa conformité au Règlement ; et d'autre part, collecter et traiter, par défaut, exclusivement les données à caractère personnel strictement nécessaires à la finalité poursuivie par le traitement ;

- the obligation to document all of the personal data processing activities the companies perform.

- l'obligation de documenter l'ensemble des traitements des données personnelles effectuées au sein des entreprises.

INTRODUCTION

La question des données qui, il y a encore quelques années était une question pour techniciens, est devenue aujourd'hui une question pour tous les décideurs, tous les acteurs de la vie publique et de la sphère économique, et assurément pour tous les juristes. La numérisation est en effet devenue omniprésente et le risque cyber se manifeste dans tous les domaines. Il suffit pour s'en convaincre de rappeler que l'on « hacke » des entreprises, des administrations, des hôpitaux, des particuliers, etc.[7]

Par ailleurs, les individus sont de plus en plus soucieux de la protection de leurs données. L'exemple le plus emblématique est sans doute l'affaire dite *Max Schrems*, qui a donné lieu à un retentissant arrêt de la Cour de justice de l'Union européenne.[8] Dans cette affaire, Maximillian Schrems, étudiant autrichien et utilisateur de Facebook, réprouvait le transfert des données qu'il fournissait à Facebook depuis la filiale irlandaise de la société vers des serveurs situés aux Etats-Unis, données qui faisaient ensuite l'objet d'un traitement. Il avait alors déposé une plainte auprès de l'autorité irlandaise de contrôle, estimant qu'au regard des révélations faites en 2013 par Edward Snowden au sujet des activités des services de renseignement des Etats-Unis, le droit et les pratiques des Etats-Unis n'offraient pas de protection suffisante contre la surveillance, par les autorités publiques, des données transférées vers ce pays.[9] L'autorité irlandaise avait rejeté la plainte au motif, notamment, que dans sa décision du 26 juillet 2000, la Commission avait considéré que dans le cadre du régime dit de la « sphère de sécurité » (*safe harbor*) les Etats-Unis assuraient un niveau adéquat de protection aux données à caractère personnel transférées. Saisie d'une question préjudicielle par la High Court of Ireland, la Cour de justice de l'Union européenne a estimé que les autorités nationales de contrôle pouvaient, même en présence d'une décision de la Commission constatant qu'un pays tiers offre un niveau de protection adéquat des données personnelles, examiner si le transfert des données d'une personne vers ce pays respecte les exigences de la législation de l'Union relative à la protection de ces données, et saisir les juridictions nationales, au même titre que la personne concernée, afin qu'elles procèdent à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision. La Cour de justice a du même coup invalidé la décision de la Commission constatant que les Etats-Unis assuraient un niveau de protection adéquat aux données à caractère personnel transférées.

L'affaire n'est pas close, car le 3 octobre 2017, la High Court of Ireland a de nouveau interrogé la Cour de justice de l'UE sur la validité du mécanisme des clauses contractuelles types, lesquelles encadrent le transfert de données entre

INTRODUCTION

The data question, a few years ago only an issue for technicians, has now become one that concerns all decision-makers, all those involved in public life and the economic sphere, and certainly all jurists. Digitisation has now become pervasive and cyber risk is present in all arenas. To find proof of this, one only needs to observe how companies, administrations, hospitals, individuals, etc. have become victims of cyber-attacks.

Furthermore, individuals are increasingly concerned about the protection of their data. Perhaps the most emblematic example of this is the case known as *Max Schrems*, which led to the momentous ruling by the Court of Justice of the . In this case, Maximiliam Schrems, an Austrian student and Facebook user, denounced the transfer of the data he provided to Facebook from the company's Irish subsidiary to servers located in the US, where the data was processed. He then filed a complaint with the Irish Data Protection Commissioner, believing that in light of the revelations made in 2013 by Edward Snowden about the activities of the US intelligence services, US law and practices did not offer sufficient protection against the monitoring of the data transferred to that country by public authorities. The Irish authority dismissed the complaint on grounds that in its decision of 26 July 2000, the Commission had considered that in the framework of the so-called ''Safe Harbour'' system, the US provided an adequate level of protection for the personal data that was transferred there. In light of reference made to a preliminary ruling by the High Court of Ireland, the Court of Justice of the European Union found that the national supervisory authorities could, even with the existence of a decision by the Commission stating that a third country offered an adequate level of protection of personal data, examine whether the transfer of a person's data to this country respected the requirements of EU legislation on the protection of this data. It also found that they could also bring the case before the national courts, in the same manner as the person in question, in order to refer it for a preliminary ruling to review the validity of this decision. At the same time, the Court of Justice overturned the decision of the Commission that found that the US provided an adequate level of protection for the personal data that was transferred there.

This is not a closed case, however, because on 3 October 2017, the High Court of Ireland again questioned the Court of Justice of the EU on the validity of the mechanism of standard contractual clauses, which govern the transfer of data between the EU and the US.

It is therefore evident that individuals are calling for increased protection of their personal data by European authorities, which are implementing stricter control.

l'Union européenne et les Etats-Unis.[10] Il est ainsi manifeste que les individus réclament plus de protection de leurs données personnelles auprès des autorités européennes, qui opèrent donc un contrôle plus rigoureux.

Finally, the issue of personal data became a subject of major concern for companies with the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, known as the General Data Protection Regulation on the protection of data (hereinafter, GDPR). This Regulation provides for potential sanctions of 4 per cent of the companies' consolidated global turnover in the event of their failure to meet its obligations.

Enfin, la question des données personnelles devient un sujet de préoccupation majeur pour les entreprises avec l'adoption du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit Règlement général sur la protection des données (ci-après RGPD).[11] Celui-ci prévoit en effet des sanctions potentielles à hauteur de quatre pour cent du chiffre d'affaires mondial consolidé des entreprises en cas de manquement à leurs obligations découlant du Règlement.

Although the GDPR entered into force on 24 May 2016, its effects, and in particular the attendant sanctions, have been deferred until 25 May 2018 in order to provide organisations with sufficient time to become compliant. Companies therefore have only a few months remaining to comply with the GDPR. Yet, in October 2017 some barometers predicted that ''81% of enterprises will not be in compliance by May 2018''.

Si le RGPD est entré en vigueur le 24 mai 2016, ses effets, et notamment les sanctions, ont été différés au 25 mai 2018 afin de laisser aux organisations le temps de se mettre en conformité.[12] Il ne reste donc que quelques mois aux entreprises pour se mettre en conformité avec le RGPD, tandis que certains baromètres prédisent en octobre 2017 que « 81% des entreprises ne seront pas en conformité en mai 2018 ».[13]

The GDPR is bringing about a real cultural revolution within companies by forcing them to consider risks to other people, whereas traditionally they only considered their own risks. Thus the GDPR makes impact assessments mandatory whenever data processing is ''likely to result in a high risk for the rights and freedoms of individuals''.

Le RGPD opère une véritable révolution culturelle au sein des entreprises en les obligeant à penser les risques pour les personnes, alors que traditionnellement elles pensaient les risques pour elles-mêmes.[14] Le RGPD rend ainsi obligatoire les analyses d'impact dès lors qu'un traitement de données est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».[15]

Furthermore, what is of particular interest here is that the GDPR changes the ''toolbox'' and induces a shift in the data regulation paradigm. We are moving from a system of authorisations granted by regulators, with sanctions that were not very significant for large companies, to a system without authorisations in which the sanctions are potentially substantial, and within which the accountability of the company plays a decisive role. Therefore, the major change introduced by the GDPR lies in the switch from compliance being monitored exclusively by the CNIL (exo-control) to a control that is also carried out by the company itself (endo-control).

Par ailleurs, et pour ce qui nous intéresse plus particulièrement, le RGPD change la « boîte à outils » et le paradigme de la régulation des données. D'un système d'autorisations données par des régulateurs et avec des sanctions peu significatives pour les grandes entreprises, on passe à un dispositif sans autorisations, où les sanctions sont potentiellement considérables et au sein duquel la responsabilisation des entreprises (*accountability*) joue un rôle décisif. Le changement majeur apporté par le RGPD réside ainsi dans le passage d'un contrôle de conformité à la loi exclusivement effectué par la CNIL (exocontrôle) à un contrôle également opéré par l'entreprise elle-même (endocontrôle).

In exchange for this freedom (the new scheme is no longer based on a system of prior formalities), the European legislation imposes an accountability principle on companies. This concept is introduced in art.5, para.2 of the GDPR, which states that:

En échange de cette liberté (le dispositif actuel ne repose plus sur un système de formalités préalables), le législateur européen impose un principe d'*accountability*, c'est-à-dire de responsabilisation des entreprises.[16] Cette notion est introduite à l'art.5, s.2 du RGPD, lequel énonce que

> « le responsable du traitement est responsable du respect du paragraphe 1 [qui établit la liste de plusieurs principes généraux relatifs au traitement des données] et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

> ''the controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 [which establishes the list of several general principles for processing data] (accountability)''.

L'*accountability*, au sens du Règlement, est donc une situation dans laquelle l'entreprise est capable de démontrer qu'elle agit en conformité avec les principes du Règlement. L'article 24, intitulé « Responsabilité du responsable du traitement », réitère l'obligation de démontrer la conformité, laquelle doit passer par la mise en place de « mesures techniques et organisationnelles appropriées pour s'assurer — et être en mesure de démontrer — que le traitement est effectué conformément au présent règlement ».

Accountability, within the meaning of the Regulation, is a situation in which the company is able to demonstrate that it complies with the principles of the Regulation. Article 24, entitled ''Responsibility of the controller'', reiterates the obligation to demonstrate compliance, which must include the implementation of ''appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.''

En d'autres termes, en vertu du principe d'*accountability*, les entreprises devront, d'une part, être capables de prendre elles-mêmes des mesures — techniques, organisationnelles et juridiques — pour se conformer au droit des données personnelles, et d'autre part, être en mesure de démontrer leur conformité à tout moment.

In other words, under the accountability principle, companies must on the one hand be able to take measures—technical, organisational and legal—on their own to comply with personal data law, and on the other hand be able to demonstrate their compliance at any given time.

Le RGPD se borne cependant à fixer un cadre général, sans déterminer les moyens concrets de mise en œuvre de ce principe, qui devront nécessairement être déclinés au cas par cas. La question se pose dès lors de savoir quels changements les entreprises vont devoir opérer pour se mettre en conformité avec le RGPD. En d'autres termes, quelles sont les mesures à prendre pour mettre en œuvre ce nouveau processus d'autorégulation ?

However, the GDPR only sets a general framework, without determining the specific means of implementing this principle, which must necessarily be determined on a case-by-case basis. This prompts the question of what changes companies will have to make to become compliant with the GDPR. In other words, what measures will need to be taken to implement this new self-regulation process?

Parmi les différents chantiers à mettre en œuvre, trois axes principaux se dessinent. Ils seront traités dans les développements qui vont suivre. Le premier tient à la désignation d'un délégué à la protection des données. Le second est lié à l'obligation de protéger les données dès la conception — d'un produit ou d'un service — et par défaut. Enfin, le troisième impose aux entreprises l'obligation de tenir un registre des traitements des données effectués en leur sein.

Among the various measures to be implemented, three main focuses are emerging. They will be addressed in the following sections. The first is the appointment of a data protection officer. The second is related to the obligation to protect data as early as the product or service design stage, and by default. Finally, the third requires companies to keep a record of the data processing activities they carry out.

LA DESIGNATION OBLIGATOIRE D'UN DELEGUE A LA PROTECTION DES DONNEES

THE COMPULSORY APPOINTMENT OF A DATA PROTECTION OFFICER

Le RGPD prévoit la désignation obligatoire d'un délégué à la protection des données (« *Data Privacy Officer* » ou « DPO ») dans plusieurs cas, et notamment lorsque :

The GDPR provides for the compulsory appointment of a Data Protection Officer (DPO) in several cases, particularly in any case where:

- « les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et

- ''the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and

systematic monitoring of data subjects on a large scale; or

- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10''.

systématique à grande échelle des personnes concernées ; ou

- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9[17] et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».[18]

A new stakeholder has therefore entered the company, with a significant role, since ''the Data Protection Officer shall directly report to the highest management level of the controller or the processor''.

Un nouvel acteur fait ainsi son apparition au sein de l'entreprise, avec un message fort, puisque « le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ».[19]

This appointment will lead to various difficulties in practice, depending on the initial maturity of the company in terms of data governance, and the company's type of structure and business sector.

Cette désignation suscitera des difficultés diverses en pratique, selon la maturité initiale de l'entreprise en matière de gouvernance des données, le type de structure et le secteur d'activité de l'entreprise.

While some companies have already appointed a CNIL-recognised data protection officer (hereinafter CIL, for the French term *Correspondant Informatique et Libertés*), others do not have this position or have limited the CIL's activity to a restricted scope (for example, human resources management).

En effet, alors que certaines entreprises ont déjà désigné un Correspondant Informatique et Libertés (ci-après CIL),[20] d'autres n'en sont pas dotées ou ont circonscrit l'activité du CIL à un périmètre restreint (la gestion des ressources humaines, par exemple).

In the first instance, the Data Protection Officer is ideally suited to replace the CIL since they have similar functions. We know that the CIL's role is to ensure that an organisation complies with the Act of 6 January 1978 on Information Technology, Data Files and Civil Liberties (hereinafter, Data Protection Act). In other words, the CIL is the reference person for all questions regarding privacy policy within the company, as well as being the primary contact person for communications with the CNIL. The DPO, on the other hand, is responsible for ensuring that the organisation which has appointed him or her is compliant with the GDPR. The CNIL presents this role as the ''conductor whose mission involves providing information, advice and internal control''. More specifically, in accordance with art.39, para.1 of the GDPR, the DPO primarily has the following responsibilities:

Dans le premier cas, le délégué à la protection des données a une vocation naturelle à succéder au CIL dans la mesure où leurs fonctions sont similaires. On sait en effet que le rôle du CIL consiste à veiller à la conformité d'une organisation à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés).[21] En d'autres termes, le CIL est non seulement le référent pour toute question ayant trait au respect de la vie privée au sein de l'entreprise, mais il est également l'interlocuteur privilégié de la CNIL. Le DPO est quant à lui chargé de mettre en œuvre la conformité au RGPD au sein de l'organisme qui l'a désigné.[22] Il est présenté par la CNIL comme le « chef d'orchestre qui exerce une mission d'information, de conseil et de contrôle en interne ».[23] Plus précisément, et conformément à l'art.39, para.1 du RGPD, le DPO est principalement chargé :

- to inform and advise the controller or the processor and their employees on the content of the new obligations;

- d'informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés sur le contenu des nouvelles obligations ;

- to ensure the proper application of the GDPR and to monitor compliance. Therefore, ''the CIL is no longer responsible for informing the data controller in the event of breaches, but must now guarantee the compliance of actions carried out within the organisation'';

- de contrôler le respect et la bonne application du RGPD. Ainsi, « il ne s'agit plus pour le CIL d'informer le responsable de traitement en cas de manquements, mais de se placer en garant de la conformité des actions entreprises au sein de l'organisme »[24] ;

- to advise the organisation on how to proceed with data protection impact assessments, and to monitor their performance. The Regulation

- de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution. Les études d'impacts sont en effet

rendues obligatoires par le Règlement dans le cas d'un traitement de données qui comporterait un risque élevé d'atteinte aux droits et libertés des individus ;

- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Pour autant, le CIL d'aujourd'hui ne deviendra pas automatiquement le délégué à la protection des données de demain. Le RGPD confère en effet une autre dimension au délégué.

En premier lieu, les missions du délégué, et tout particulièrement son rôle de conseil et de sensibilisation sur les nouvelles obligations du Règlement, sont renforcées. A cet égard, la sensibilisation du personnel de l'entreprise — de la direction aux chefs de projet — sera délicate dans les entreprises où la donnée n'est pas au cœur du métier, et où le « retour sur investissement » peut sembler minime. Une véritable implication de l'ensemble du personnel en matière de protection des données sera illusoire tant que la direction ne prendra pas des mesures en ce sens et ne donnera pas l'exemple.

En tout état de cause, le délégué sera mieux armé que le CIL pour exercer ses missions dans la mesure où le RGPD fait obligation de lui donner les ressources nécessaires, notamment en termes de budget et d'infrastructures.[25]

En deuxième lieu, dans la mesure où le délégué doit rendre compte au plus haut niveau de la direction de l'entreprise,[26] et ainsi délivrer son expertise aux cadres dirigeants, sa fonction se professionnalise. La question de ses qualifications et de sa formation se posera avec davantage d'acuité. En effet, alors que la loi dite Informatique et Libertés prévoit que le CIL « est une personne bénéficiant des qualifications requises pour exercer ses missions »,[27] le RGPD va plus loin en énonçant que :

> « le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 ».[28]

De fait, de plus en plus d'universités notamment en France[29] et en Europe[30] proposent des formations de second cycle alliant le droit et les nouvelles technologies. Pour autant, en pratique, la formation continue se révèle la plus adaptée. En effet, pour exercer efficacement ses missions, le délégué doit, d'une part, être capable de comprendre les opérations de traitement effectuées par l'organisme qui l'a désigné, et d'autre part, avoir une connaissance intime de cet organisme et de son secteur d'activité.[31]

makes impact assessments mandatory when the processing of data involves a high risk for the rights and freedoms of individuals;

- to cooperate with the supervisory authority and to act as the contact point for this authority.

However, the current CIL will not automatically become the future data protection officer. The GDPR confers an additional dimension on this officer.

First of all, the DPO's position involves more duties, including the role of advising and raising awareness on the new obligations of the Regulation. In this regard, raising awareness among the company's staff—from senior management to project leaders—will be difficult in companies for whom data is not part of the core business, and for whom the ''return on investment'' may seem minimal. Genuine involvement of all staff in the area of data protection would be unrealistic unless senior management takes steps in this direction and leads by example.

In any event, the DPO will be better equipped than the CIL to carry out their duties, since the GDPR stipulates that these officers must be given the necessary resources, particularly in terms of budget and infrastructure.

Secondly, since the DPO must report to the highest level of company management, and thus offer their expertise to senior executives, this role takes on a higher level of professionalism. The question of the individual's training and qualification becomes more significant. Whereas the Data Protection Act stipulates that the CIL ''must be an individual who holds the qualifications required to carry out his or her duties,'' the GDPR goes a step further, stating that:

> ''the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39''.

As a result, more and more universities in France and Europe are offering graduate training courses that combine law and new technologies. Yet, in practice, continuing education courses are better suited to this position. To effectively carry out these tasks, the DPO must on the one hand be able to understand the processing operations carried out by the organisation that appointed him or her, and on the other hand have an in-depth understanding of the organisation and its business sector.

Finally, the Data Protection Officer position will likely involve a more strategic aspect than the CIL position. The officer will need to independently challenge the business departments and have a sufficiently strong profile capable of questioning, where appropriate, company projects of strategic importance related to big data or digital marketing. To this end, the GDPR stipulates that:

> ''the controller and processor shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks.''

Therefore, if a DPO considers that a processing operation will likely pose a high risk and advises the controller to carry out an impact assessment, and if the processor disagrees with the DPO's analysis, the DPO may not be removed from his or her position for having provided this advice. Similarly, pursuant to art.38 para.6 of the GDPR, ''the controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.'' This means that the officer must not have a position within the organisation that would involve him or her determining the purposes or means of the processing of data.

The task of integrating and positioning the DPO within a company is more difficult within large, hierarchical structures, as well as in sectors in which data is central to the business, such as banks and insurance companies. In practice, reflections on the kind of role the DPO should play can lead to significant delays. Should it be connected to the admin department, the legal department, the IT department or the communications department? None of these positions are completely suited to this role due to the multiple skills the DPO must possess: legal, technical and communication skills. For example, in some banks the DPO reports to the ''compliance'' department. It is perhaps regrettable that some approaches simplify this role, and do not reflect the true challenge the GDPR represents.

The task of positioning the DPO is less problematic within smaller structures and in the industry sector, in which data is not as significantly linked to the core business. The issue then becomes polarised, focusing on the efficiency of its function rather than on the strategies for managerial positioning.

Finally, while the designation of a CIL was optional, in some cases the compulsory appointment of a data

Enfin, le poste de délégué à la protection des données est susceptible de revêtir une dimension plus stratégique que celui du CIL. Le délégué doit en effet pouvoir, en toute indépendance, interpeller les directions métiers et avoir la stature suffisante pour remettre en question, le cas échéant, des projets d'entreprise à fort enjeu liés au *big data* ou au marketing digital. A cette fin, le RGPD prévoit que :

> « le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions ».[32]

Ainsi, si un DPO estime qu'un traitement est susceptible d'engendrer un risque élevé et conseille au responsable de traitement de procéder à une analyse d'impact, et si le responsable de traitement est en désaccord avec l'analyse du DPO, alors ce dernier ne peut être relevé de sa fonction pour avoir formulé un tel conseil.[33] De même, en application de l'art.38 para.6 du RGPD, « le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts ». Cela signifie que le délégué ne peut occuper au sein de l'organisme des fonctions le conduisant à déterminer les finalités et les moyens d'un traitement.[34]

La question de l'intégration et du positionnement du délégué au sein d'une entreprise est davantage sensible dans les grandes structures très hiérarchisées, ainsi que dans les secteurs où la donnée est au cœur du métier, comme la banque ou les assurances. En pratique, d'importants retards peuvent résulter d'une réflexion sur la place que devra occuper le délégué. Faut-il le rattacher au secrétariat général, au service juridique, au service IT ou au service communication ? Aucune de ces positions n'est réellement satisfaisante en raison des multiples compétences attendues du délégué : compétences juridiques, techniques et de communication. A titre d'exemple, dans certaines banques, le délégué est rattaché au service « conformité ». On peut regretter certaines approches réductrices, alors que l'enjeu véritable du RGPD réside ailleurs.

La question du positionnement du délégué est moins problématique dans les plus petites structures ou dans le secteur de l'industrie où la donnée n'est pas aussi sensiblement liée au cœur du métier. L'enjeu est alors polarisé autour de l'efficacité de sa fonction plutôt que sur des stratégies de positionnement managérial.

Enfin, alors que la désignation d'un CIL était facultative, la désignation obligatoire d'un délégué à la protection des

données dans certaines hypothèses opère un changement d'échelle. Ce sont en effet plus de 28.000 postes de délégué qui sont à pourvoir au sein de l'Union européenne[35] et la pénurie frappe la France, au même titre que d'autres Etats membres de l'Union européenne.[36] Certains Etats membres, qui ne connaissent pas la fonction de CIL, sont au demeurant davantage pénalisés.

protection officer will now require a scale-up. There are indeed over 28,000 DPO posts to be filled within the EU and the shortage has affected France as well as other Member States of the EU. Some Member States that did not have the CIL function are further penalised.

La question du recrutement d'un délégué à la protection des données est donc particulièrement préoccupante. A cet égard, plusieurs possibilités s'offrent aux entreprises.

Hiring a Data Protection Officer therefore represents a major concern. To meet this challenge, companies have several options.

Tout d'abord, il ne faut pas négliger les candidats internes, quand bien même la tentation peut être grande de vouloir recruter un expert venant de l'extérieur. En pratique, en effet, on attend du délégué une connaissance intime de l'entreprise et d'excellentes qualités de communication. Un expert — juridique ou informatique — recruté à l'extérieur ne sera en revanche pas connu au sein de l'entreprise et pourra éprouver des difficultés à vulgariser auprès du plus grand nombre des informations spécialisées. Un choix astucieux pourrait alors consister à former quelqu'un en interne. A cet égard, les RSSI ou les auditeurs internes incarnent de bons candidats.

First of all, they must not overlook internal candidates, even when it is tempting to seek an outside expert. In practice, the DPO is expected to have in-depth knowledge of the company and excellent communication skills. However, a legal or IT expert recruited from outside the company will not be well known within the company and may have difficulties communicating specialised information to as many staff members as possible. Training an internal staff member could therefore be a wise choice. In this case, information systems security managers and internal auditors could be good candidates.

Ensuite, le délégué à la protection des données peut être mutualisé, c'est-à-dire désigné pour plusieurs organismes, sous certaines conditions. Par exemple, lorsqu'un délégué est désigné pour un groupe d'entreprises, il doit être facilement joignable à partir de chaque lieu d'établissement. Il doit en effet être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec l'autorité de contrôle.[37]

The Data Protection Officer may also share his or her expertise with several organisations under certain conditions. For example, when a DPO is appointed for a group of companies, he or she must be reachable from each entity. The DPO must be able to communicate effectively with the individuals concerned and cooperate with the supervisory authority.

Enfin, le RGPD permet aux entreprises d'externaliser les délégués à la protection des données. L'article 37 para.6 dispose en effet que « le délégué à la protection des données peut [...] exercer ses missions sur la base d'un contrat de service ». Toutefois, si l'idée d'externaliser les délégués est régulièrement évoquée,[38] une telle initiative ne semble réellement opératoire que dans des petites structures, telles des *start-ups* innovantes qui réalisent des projets risqués pour la vie privée.

Finally, the GDPR allows companies to outsource Data Protection Officers. Article 37 para.6 states that ''The Data Protection Officer may [...] fulfil the tasks on the basis of a service contract.'' However, although the idea of outsourcing the DPO is often mentioned, this kind of initiative only seems feasible for small structures, such as innovative start-ups that develop projects that involve privacy risks.

GARANTIR LA PROTECTION DES DONNEES DES LA CONCEPTION (*PRIVACY BY DESIGN*) ET PAR DEFAUT (*PRIVACY BY DEFAULT*)

ENSURING DATA PROTECTION THROUGH PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

La protection des données dès la conception est prévue à l'art.25 du RGPD. Il s'agit d'une démarche proactive en vertu de laquelle les responsables de traitement et les sous-traitants doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer, dès le stade de développement ainsi que tout au long du cycle de vie d'un produit, d'un service, d'une application ou d'une

Data protection by design is provided for in art.25 of the GDPR. It is a proactive approach in which the controller and processors must implement suitable technical and organisational measures to ensure, from the development stage and throughout the life cycle of a product, service, application or solution, its compliance with the GDPR, and especially the protection of the rights of data subjects. In other words, the GDPR

imposes an obligation to anticipate all the risks involved in processing personal data.

solution, sa conformité au RGPD, et tout particulièrement la protection des droits des personnes concernées.[39] En d'autres termes, le RGPD impose une obligation d'anticipation de tous les risques liés au traitement des données à caractère personnel.

More generally, the Privacy by Design measure is a question of common sense, effectiveness and efficiency. The ex-post costs of compliance can indeed be very high if a breach or non-compliance is detected after the production of an application.

Plus généralement, le *Privacy by Design* est une mesure de bon sens, d'efficacité et d'efficience. Les coûts de mise en conformité *a posteriori* en cas de découverte de failles ou de non-conformité après la mise en production d'une application peuvent en effet se révéler très élevés.

Protection of data by default, on the other hand, involves the default collection and processing only of personal data that is strictly necessary for the purpose of the processing operation. The GDPR specifies that data protection by default limits the amount of personal data collected, as well as the scope of the processing, how long the data is kept and the amount of people who can access the data.

La protection des données par défaut, consiste quant à elle à collecter et traiter, par défaut, exclusivement les données à caractère personnel strictement nécessaires à la finalité poursuivie par le traitement. Le RGPD précise que la protection des données par défaut vise à limiter la quantité de données à caractère personnel collectées, ainsi que l'étendue du traitement, la durée de conservation des données et le nombre de personnes pouvant accéder aux données.[40]

These measures must ''make the individual master of his or her data'' and thus enable ''the company to adopt a responsible approach that boosts user confidence and offers a competitive advantage''.

Ces mesures doivent « rendre l'individu maître de ses données »[41] et permettre ainsi à « l'entreprise de s'inscrire dans une démarche responsable améliorant la confiance des utilisateurs et apportant un avantage compétitif ».[42]

To better understand the concept of Privacy by Design, which appears in the text of the GDPR, we must present the work of the woman who inspired it, Canadian Ann Cavoukian, who conceptualised it in the 1990s during her term as the Information and Privacy Commissioner of Ontario. She began with the observation that the legal framework was insufficient to ensure the true protection of privacy. She suggested that it was necessary to intervene prior to data processing by using an approach that integrates technical and organisational measures into all technology in order to avoid the invasion of individuals' privacy. Ann Cavoukian identified several principles that should govern Privacy by Design:

Pour mieux saisir le concept de *Privacy By Design*, qui fait son apparition textuelle dans le RGPD, il faut présenter les travaux de son inspiratrice, la canadienne Ann Cavoukian, qui l'a conceptualisé dans les années 90 alors qu'elle était commissaire à l'information et à la protection de la vie privée de l'Ontario. Celle-ci est partie du constat selon lequel le cadre légal était insuffisant pour assurer une réelle protection de la vie privée. Selon elle, il fallait intervenir en amont grâce à une démarche qui intègre à toute technologie des mesures techniques et organisationnelles afin qu'elle ne porte pas atteinte à la vie privée des individus. Ann Cavoukian a identifié divers principes devant régir le *Privacy By Design*[43] :

- *Proactivity*, which aims to prevent personal data breaches rather than trying to rectify the consequences after the fact. In this regard, the economic operator must think about the privacy breach incidents that could result from the exploitation of the technology. The difficulty here is related to the fact that the economic operator must examine this issue in the short, medium and long terms, even though all the potential incidents cannot always be anticipated;

- *La proactivité*, qui consiste à prévenir les risques d'atteinte aux données personnelles plutôt que d'essayer d'en corriger les conséquences *a posteriori.* A cet égard, l'opérateur économique doit s'interroger sur les incidents d'atteinte à la vie privée qui peuvent résulter de l'exploitation de la technologie. La difficulté ici va être liée au fait que l'opérateur économique doit se poser la question à court, moyen et long terme, alors même que l'ensemble des incidents possibles ne peut pas toujours être anticipé ;

- *Protection by default*, in order to protect individuals' personal data in all circumstances, without requiring any action on their part. This means that the operator must define the maximum level of protection and ensure that

- *La protection par défaut*, afin de protéger les données personnelles de l'individu en toutes circonstances, même sans action préalable de sa part. Cela signifie que l'opérateur doit définir le niveau de protection

maximale et s'assurer que la solution technique la garantit sans qu'aucun réglage par l'utilisateur ne soit nécessaire ;

- *La protection par construction*, qui suppose d'intégrer la protection de la vie privée dans la conception des systèmes et des pratiques. Ainsi, la réflexion de la protection de la vie privée doit être prise en compte dès la conception du produit ou du service. Ce principe vise également à concilier les intérêts des utilisateurs d'un produit et des entreprises ;
- *La protection de bout en bout*, pendant toute la période de conservation des renseignements. Cette obligation n'est pas nouvelle et suppose que l'entreprise soit en mesure d'assurer la sécurité de la conservation et de la destruction des données ;
- *Visibilité et transparence*, qui devront être assurées par une documentation réalisée par le responsable de traitement afin de démontrer, notamment en cas de contrôle, que l'utilisation de la technologie est conforme à ses objectifs ;
- *Souveraineté de l'utilisateur*, dont le respect de la vie privée et la protection des données personnelles doivent structurer les échanges d'information.

Ces principes fondamentaux doivent permettre de réduire les risques pour les personnes, liés à un mauvais usage de leurs données, ce qui n'était pas assuré par le régime de formalités préalables.

En pratique, le *Privacy By Design* se pense *in concreto*, en fonction de chaque modèle technique et commercial développé, et repose sur une analyse des risques adaptée, qui durera tout au long de la vie du produit/service. De ce point de vue, la généralité des termes employés par le RGPD est source d'interrogations. Se pose en particulier la question des acteurs qui doivent prendre part au respect de ce principe, des technologies concernées et surtout des mesures concrètes à mettre en œuvre.[44]

Les acteurs du Privacy By Design. Dans la mesure où ce principe est à la frontière d'obligations juridiques, informatiques, économiques, éthiques et organisationnelles, il va nécessiter une coopération de l'ensemble des acteurs de l'entreprise. L'entreprise va devoir insuffler une véritable culture des données personnelles à l'ensemble des intervenants. Si cette culture devra être portée en premier lieu par le *Data Privacy Officer*, on comprend aisément que les responsables de développement et de projet vont devoir être les premiers à s'emparer du *Privacy By Design* et à en tenir compte dès le stade de réflexion sur le développement de nouvelles technologies.

the technical solution guarantees this level without requiring the user to make any adjustments;

- *Protection embedded into design*, which requires the protection of privacy to be integrated into the design stage of systems and practices. The reflection on privacy protection must therefore begin at the design stage for a product or service. This principle also aims to reconcile the interests of the users of a product with those of companies;
- *End-to-end security*, throughout the entire period the information is retained. This obligation is not new and assumes that the company is able to ensure the security of data retention and destruction;
- *Visibility and transparency*, which must be ensured through documentation carried out by the controller in order to demonstrate, particularly in the event of a control, that the use of the technology is consistent with its objectives;
- *User sovereignty*, including respect for user privacy and the protection of personal data, must structure the exchange of information.

These fundamental principles are intended to reduce the risks for individuals related to the misuse of their data, which was not provided for in the previous system of formalities.

In practice, Privacy by Design must be thought of in concrete terms, according to each technical and commercial model developed, and based on a suitable risk analysis that will continue throughout the entire life cycle of the product/service. In this regard, the general nature of the wording used in the GDPR raises questions. In particular, questions arise regarding the actors that should be involved in enforcing this principle, the technology concerned, and especially the concrete measures to be implemented.

The actors involved in Privacy by Design. Since this principle overlaps legal, IT, economic, ethical and organisational obligations, it will require the cooperation of all the company stakeholders. The company will need to instil a genuine culture of personal data protection among all stakeholders. While this culture must be primarily led by the Data Privacy Officer, it is easy to see that development and project leaders will have to be the first to integrate Privacy by Design and take it into account as early as the initial reflection process for developing new technology.

The technology concerned. Examples include social networks, devices related to e-health (watches, pedometers, etc.), connected objects such as cars (geolocation, recording behaviours), the development and use of drones, etc.

Les technologies concernées. On peut par exemple citer les réseaux sociaux, les appareils en lien avec l'e-santé (montres, podomètres, etc.), les objets connectés tels que les voitures (géolocalisation, enregistrement des comportements),[45] le développement de l'usage des drones, etc.

The measures to be implemented. In general, Privacy by Design will require companies to change their methodology for project management and will require them to make certain choices, particularly in limiting the offer they propose to customers. More specifically, this can involve, in the beginning stages of designing a personal data collection form, adding a check box to obtain the individual's consent to use their data that is not strictly necessary for the purpose for which it is being processed, and that will be used for other purposes, such as profiling for the purpose of commercial prospecting. It may also involve, at the time of a website's initial construction, planning for an area in the graphical user interface where a specific information statement will be displayed on the site. In particular, this will include all measures to anonymise or pseudo-anonymise personal information, for example, in order to limit access to aggregated data only, not to raw data when data are communicated to third parties, or to minimise the amount of data collected by a connected object according to the purpose of the processing.

Les mesures à mettre en œuvre. De manière générale, le *Privacy By Design* va obliger les entreprises à modifier leur méthodologie de gestion de projets et va les contraindre à faire des choix, notamment en restreignant l'offre qu'elles proposent à leurs clients. Plus concrètement, il peut s'agir de prévoir, dès l'élaboration d'un formulaire de collecte de données à caractère personnel, une case à cocher afin de recueillir le consentement de la personne concernée pour la collecte de ses données qui ne seraient pas strictement nécessaires à la réalisation de la finalité du traitement et qui poursuivraient d'autres finalités telles que le profilage à des fins de prospection commerciale. Il peut également s'agir de prévoir un emplacement pour la mention d'information sur l'interface graphique d'un site internet dès sa construction. Il s'agira notamment de toutes mesures d'anonymisation ou de pseudonymisation pour, par exemple, limiter l'accès aux seules données agrégées et non aux données brutes lors de leur communication à des tiers, ou encore de la minimisation de la quantité de données collectées par l'objet connecté au regard de la finalité du traitement.[46]

Beyond these uncertainties, a few difficulties may arise during the practical implementation of this concept. For example, how can a controller be sure that a given technology complies with the Privacy by Design principle, especially regarding the anonymisation technique used, since it has been demonstrated that anonymisation techniques are not fool-proof and that individuals can potentially be re-identified by cross-referencing several anonymised datasets?

Au-delà de ces incertitudes, quelques difficultés peuvent surgir dans la mise en œuvre pratique de ce concept.[47] Ainsi, comment un responsable de traitement peut-il être sûr qu'une technologie est conforme au principe de *Privacy By Design* d'autant, que concernant la technique de l'anonymisation par exemple, il a été démontré que la plupart des techniques d'anonymisation n'étaient pas infaillibles et qu'il était possible de ré-identifier des personnes physiques via un croisement de plusieurs données anonymisées ?[48]

Moreover, the fundamental principles of Privacy by Design appear contrary to the very operating principle of certain technologies: for example, how can data be minimised based on the given objective in the case of Big Data, when its very purpose is to process huge volumes of data for an objective that it is meant to discover on its own?

Les principes fondamentaux de la *Privacy By Design* semblent par ailleurs contraires au principe même de fonctionnement de certaines technologies : comment minimiser les données à l'accomplissement d'un objectif alors que, par exemple, le *Big Data* trouve sa raison d'être dans le traitement de volumes gigantesques de données dans un dessein qu'il est censé découvrir lui-même ?[49]

Finally, it is extremely difficult to anticipate all the potential uses related to changes in behaviours and in the initial technology. A possible solution could involve an ex-post intervention, using an approach that some call Privacy by Redesign, which would be aimed at applying the fundamental Privacy by Design principles to existing systems.

Enfin, il est extrêmement difficile d'anticiper tous les usages, qui peuvent être liés tant à l'évolution des comportements qu'à la technologie initiale. Une intervention *a posteriori* en application d'un principe, que certains nomment *Privacy by Redesign*, qui aurait pour objectif d'appliquer les principes fondamentaux de *Privacy By Design* aux systèmes existants, pourrait être une réponse.[50]

LA TENUE D'UN REGISTRE DES TRAITEMENTS

Enfin, avec le principe d'*accountability*, les entreprises doivent être en mesure de démontrer *à tout moment* qu'elles respectent le RGPD. Pour prouver cette conformité, elles doivent tenir un registre des traitements, lequel documente, comme son nom l'indique, l'ensemble des traitements des données personnelles en leur sein.

Si cette obligation de déclarer les traitements existe depuis la loi dite Informatique et Libertés de 1978,[51] force est de constater qu'en pratique elle a peu été respectée. S'ouvre dès lors pour les entreprises un travail de fouille potentiellement titanesque dans 10, 20, 30, voire 40 ans de processus métier afin d'établir ce « *data mapping* ». Il s'agit sans conteste d'un des plus gros chantiers de la mise en conformité avec le RGPD. A cela s'ajoute la cartographie des contrats de sous-traitance, qu'il faudra le cas échéant renégocier.

Concrètement, ce dossier documentaire devra indiquer les différents traitements de données personnelles, les catégories de données personnelles traitées, les objectifs poursuivis par les opérations de traitement de données, les acteurs (internes ou externes) qui traitent ces données, les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Ainsi, le RGPD impose aux entreprises des obligations qui peuvent se révéler aussi chronophages (l'élaboration d'un registre des traitements) que coûteuses (les moyens, informatiques en particulier, pour réaliser ce registre). Pour autant, la plupart de ces obligations existaient déjà. Le RGPD se bornerait-il à les formaliser ? L'apport réel du RGPD résiderait-il ailleurs, dans la prise de conscience des enjeux liés aux traitements des données personnelles et la nécessité d'apporter des réponses uniformes à ces problèmes transnationaux ? Les avis du management et de la gouvernance sont souvent partagés.

KEEPING A RECORD OF PROCESSING ACTIVITIES

Finally, according to the accountability principle, companies must be able to demonstrate their compliance with the GDPR *at any time*. To prove this compliance, they must keep a record of processing activities which, as the name implies, records all the personal data the companies process.

While this obligation to declare processing activities existed in the Data Protection Act of 1978, it is now clear that this obligation has seldom been met. Companies now must face the potentially monumental task of searching through 10, 20, 30, or even 40 years of business processes in order to establish this ''data mapping''. This is without a doubt one of the largest operations required for compliance with the GDPR. Added to this is the mapping of subcontracting agreements, which in certain cases will need to be renegotiated.

In practical terms, this documentary record must indicate the various personal data processing activities, the categories of personal data processed, the objectives set for the data processing operations, the actors involved (internal or external) in processing this data, the data flows specifying the origin and destination of the data, especially in order to identify the possible transfers of data outside the EU.

Therefore, the GDPR imposes obligations on companies that could prove to be as time-consuming (the development of a processing record) as they are costly (the resources, especially in terms of IT, required to develop this record). And yet most of these obligations were already in existence. Has the GDPR merely formalised them? Perhaps the real benefit of the GDPR lies elsewhere, in raising awareness of the issues related to personal data processing and the need to provide consistent responses to these transnational problems? There are varying opinions on this issue among those in management and governance.

APPENDIX: PERSPECTIVE OF AN OPERATIONAL MANAGER

Olivier Rigaudy, Managing Director of the Teleperformance Group

Which changes do you need to implement within your company in order to be compliant with the GDPR? Could you please, among others, detail, depending on the activity of your company, the measures that you have taken and that you will take regarding privacy by design and privacy by default?

Teleperformance operates in 77 countries, and thus, it also operates in countries that will not be subject to the GDPR. But the Group has decided to ensure a global standard level of protection that will be based on the GDPR. To do so, the Group has applied for Binding Corporate Rules (BCRs) for both Data Controllers (when it processes the personal data of its employees, candidates, among others) and Data Processors (when the company processes personal data on behalf of its Clients). The BCRs are based on a new

Group Data Privacy Policy that will apply to each company of Teleperformance Group (whether it is located in the EEA or not).

Teleperformance has created the Privacy Office that is led by the Chief Privacy Officer and that is composed by 3 Data Privacy Officers (each responsible for the following regions: Americas (North, Central, South), CEMEA + UK, Portugal and Spain, Asia Pacific).

A specific training on the Group Data Privacy Policy will be implemented and a specific audit program to review the compliance of each subsidiary with the new Group Data Privacy Policy, the BCRs and the GDPR requirements was created.

We will ensure that the appropriate provisions set forth in the GDPR are integrated in our agreements whenever it includes a processing of personal data.

We need to ensure that each company subject to the GDPR maintains the appropriate register up-to-date with all the necessary information relating to the processing of personal data.

We already have in place an incident response process that enables us to handle fraud events or data breaches, but this incident response process will be adapted to ensure that, (i) if there is a breach of the data of our Clients' customers, we report the breach to the Client without undue delay and (ii) if there is a breach of the data of our employees, for instance, we are able to report the breach to the Supervisory Authority and the data subjects without undue delay too.

Privacy by design and by default: Teleperformance has already established a Technology Privacy Committee that aims at discovering potential information privacy issues before Teleperformance implements new processes, technologies, systems, programs, and devices.

Which difficulties do you encounter to ensure compliance with the GDPR?

Teleperformance acts as both Data Controller and Data Processor, thus we need to ensure that we are compliant with the GDPR in both scenarios.

It was a long process to proceed with the data flow mapping because Teleperformance is located in 77 countries.

We need to ensure that all the persons within the company understand the Group Data Privacy Policy (the agents, sales team, HR, management, etc...) and Teleperformance employs more than 210.000 employees around the world.

All the countries do not ensure the same level of protection (some of them provides for quite a low level), and thus, we will have to ensure that even the subsidiaries located in those countries are compliant by May 2018.

What do you think about the cultural change introduced by the GDPR (from a system of ''obligation to declare'' to the ''principle of accountability'')?

This obliges us to put in place the appropriate process and training to ensure that the companies properly maintain and update the Register on which will be detailed the processing. Indeed, the burden of proof is reversed and this is now the company that needs to prove that it is compliant, while, before it was up to the Data Protection Authority to show the non-compliance of the company, and thus the company had some time to regularise the situation. This is more stringent for the companies but this will help increase the confidence of the employees in the processing of their personal data and this will reassure our Clients when we process the personal data of their customers.

How do you see the evolution of the life of the company with the GDPR?

The GDPR will provide assurance to our employees that their personal data will be adequately protected. Regarding our Clients, on the one hand, there will be more and more discussions regarding the negotiations of the agreements and the liability provisions but we believe that the GDPR will provide assurance to our Clients that personal data of their customers is adequately protected. In addition, thanks

to the BCRs that we are implementing, this will give us flexibility to choose service locations depending on our Clients' operational needs without worrying about international data transfer laws as all the companies of the Group will provide for the same level of protection. We already conduct audits to ensure that the companies comply with the security and compliance policies that the Group implemented in 2015 in order to reduce security and fraud risks, thus the compliance with the GDPR will be integrated into the audit program. We already have a strong culture of security, thus, we are already used to aligning our processes and implementing new tools to protect personal data.

Notes

1. Associé KPMG en charge de l'activité Protection des données personnelles.

2. Président de la société KoppaSoft.

3. Avocat Associé chez McDermott Will & Emery.

4. Chief Data Officer du Groupe Figaro—CCM Benchmark.

5. Directeur Général Délégué du groupe Teleperformance.

6. Responsable Protection des Données à Caractère Personnel chez Saint-Gobain Interservices.

7. L'on se souvient à cet égard qu'en mai 2017 le « rançongiciel » *WannaCry* a été utilisé lors d'une cyberattaque mondiale touchant plus de 300.000 ordinateurs dans plus de 150 pays. Cette attaque a visé non seulement de grandes entreprises, mais également des hôpitaux et diverses administrations, en particulier au Royaume-Uni où le système informatique du National Health Service a été en grande partie paralysé. Sur l'actualité du « rançongiciel » *WannaCry*, voir le site dédié du *Monde* à l'adresse suivante : *http://www.lemonde.fr/logiciel-de-racket-wannacry/1.html* [Consulté le 13 février 2018].

8. Voir CJUE, 6 octobre 2015, *Maximillian Schrems c/. Data Protection Commissioner,* aff. C-362/14 (*Comm. com. électr. 2015, étude 21,* R. Perray et J. Uzan-Naulin ; *JCP G 2015, 1258,* A. Debet *; RLDI nov. 2015, no. 3867,* note Y. Padova ; N. Metallinos*,* « Invalidation du Safe Harbor : et après ? », *Archimag, nov. 2015*).

9. Rappelons à cet égard que la directive sur le traitement des données à caractère personnel dispose que le transfert de telles données vers un pays tiers ne peut, en principe, avoir lieu que si le pays tiers en question assure un niveau de protection adéquat à ces données (Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1995] JO L281/31. Toujours selon la directive, la Commission peut constater qu'un pays tiers assure, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection adéquat. Enfin, la directive prévoit que chaque Etat membre désigne une ou plusieurs autorités publiques chargées de surveiller l'application, sur son territoire, des dispositions nationales adoptées sur le fondement de la directive (« autorités nationales de contrôle »).

10. Voir la décision de la Irish High Court, *The Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, 2016 No. 4809 P., téléchargeable à l'adresse suivante : *https://epic.org/privacy/intl/schrems/* [Consulté le 13 février 2018].

11. Ce texte n'impose pas aux Etats membres d'abroger leur législation nationale. Ainsi, la Loi no.78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est toujours en vigueur. A cet égard, un projet de loi relatif à la protection des données personnelles a été présenté le 13 décembre 2017 en Conseil des ministres et a pour but de modifier la loi Informatique et Libertés au regard du droit de l'Union européenne.
Précisons par ailleurs que l'autorité britannique de la protection des données personnelles, l'*Information Commissioner's Office* (ICO), a indiqué que le Règlement européen entrerait en vigueur au Royaume-Uni le 25 mai 2018, comme dans l'ensemble des Etats membres de l'Union européenne. S'agissant des conséquences juridiques du Brexit sur la protection des données personnelles après le 29 mars 2019, l'ICO a d'ores et déjà précisé qu'un niveau élevé de protection des données personnelles serait maintenant au Royaume-Uni (voir *https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1625633/ico-response-implications-of-brexit-consultation-20161110.pdf* [Consulté le 13 février 2018]).

12. Voir l'art. 99 du RGPD : « 1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne. 2. Il est applicable à partir du 25 mai 2018 ».

13. Voir par ex. *https://www.globalsecuritymag.fr/Le-RGPD-81-des-entreprises-ne,20171011,74339.html* [Consulté le 13 février 2018].

14. Pour une présentation générale du RGPD, voir not. M. Griguer, « Le point sur la réforme de la réglementation européenne sur la protection des données personnelles », *Cahiers de droit de l'entreprise* no.4, juillet 2016, prat. 20 ; M. Bourgeois & F. Régnier-Pécastaing, « Le Règlement général sur la protection des données (RGPD) Un chantier à démystifier ! », *JCP éd.* G, no.36, 4 septembre 2017, p.914.

15. Article 35, para.1 du RGPD. La CNIL précise que, « généralement, les traitements qui remplissent au moins deux des critères suivants doivent faire l'objet d'une analyse d'impact :

- évaluation/*scoring* (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;

- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

Exemple : une entreprise met en place un contrôle de l'activité de ses salariés, ce traitement remplit le critère de la surveillance systématique et celui des données concernant des personnes vulnérables donc la réalisation d'un DPIA sera nécessaire » (voir le site web de la CNIL à l'adresse suivante : *https://www.cnil.fr/en/node/23907* [Consulté le 13 février 2018]).
Sur la façon de mener ces études d'impact, voir *Etude d'impact sur la vie privée (EIVP) Privacy Impact Assessment (PIA) - Comment mener une étude d'impact*, CNIL, éd. juin 2015, ainsi que les guidelines du G29 : *https://www.cnil.fr/fr/lanalyse-dimpact-relative-la-protection-des-donnees-dpia* [Consulté le 13 février 2018].

16. Sur les origines de l'*accountability*, voir W. Maxwell & S. Taïeb, « L'*accountability*, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT*, 2016, p.123. Sur ce que « du point de vue du respect des droits de l'individu, ce principe de responsabilité est sans doute plus efficace que les obligations déclaratives très lourdes qui ne faisaient pas forcément l'objet, par exemple en France, d'un contrôle de la part de la CNIL (96.323 dossiers de formalités en 2015, dont 50.339 formalités simplifiées) », voir A. Debet, « Les nouveaux instruments de conformité », *Dalloz IP/IT*, 2016, p.592.

17. C'est-à-dire « des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que [les] données génétiques, [l]es données biométriques aux fins d'identifier une personne physique de manière unique, [l]es données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».

18. Article 37, s.1 du RGPD.

19. Article 38, s.3 du RGPD : « Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ».

20. La fonction du CIL a été instaurée par le Décret no.2005-1309 du 20 octobre 2005 pris en application de la Loi no.78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

21. L'article 49 du Décret no.2005-1309 du 20 octobre 2005 prévoit que « le correspondant veille au respect des obligations prévues par la loi du 6 janvier 1978 susvisée pour les traitements au titre desquels il a été désigné ».

22. Sur l'absence de responsabilité du délégué en cas de non-respect du règlement, voir *infra* la note 36.

23. Voir le site web de la CNIL à l'adresse suivante : *https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes* [Consulté le 13 février 2018].

24. G. Péronne & E. Daoud, « L'évolution du rôle du CIL à la lumière du nouveau règlement européen sur les données personnelles », *Dalloz IP/IT*, 2016, p.192.

25. Voir l'art.38 s.2 du RGPD : « Le responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 39 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées ».

26. Voir l'art.38 s.3 du RGPD : « Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ».

27. Article 22, III de la Loi no.78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Une étude menée pour la CNIL en 2015 a montré que les CIL proviennent de domaines d'expertise très variés (profil technique à 47%, profil juridique à 19% et profil administratif à 10%) : *https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees* [Consulté le 13 février 2018].

28. Article 37 du RGPD.

29. Une nouvelle formation est proposée par l'Université Paris V Descartes pour former les DPO, le DU Protection des données à caractère personnel : *http://www.scfc.parisdescartes.fr/index.php/descartes/formations/droit/du-protection-des-donnees-a-caractere-personnel/(language)/fre-FR* [Consulté le 13 février 2018].
Sur cette formation, voir l'interview d'Anne Debet, directrice du DU, professeur de droit privé et ancien membre de la CNIL dans *La Semaine Juridique – Edition Générale* no.38, 18 septembre 2017, p.974, « Le RGPD insiste sur la nécessité de désigner un délégué à la protection des données et rend cette désignation obligatoire dans de nombreux organismes ». Elle y explique que ce DU « offre une formation à la fois généraliste et pratique. Il vise à étudier tant le cadre général de la protection des données à caractère personnel (champ d'application, principes relatifs au traitement des données, droit des personnes, obligations du responsable de traitement, rôle et pouvoirs de la CNIL...), présenté de manière concrète et pratique, que les questions plus spécifiques concernant des secteurs à forts débouchés professionnels (banque, prospection commerciale, santé, secteur public...). En outre, cette formation est pluridisciplinaire — majoritairement en droit, mais aussi en informatique (sécurité des systèmes d'information...) — ce qui est indispensable pour bien comprendre ces problématiques. »
On peut également citer le Master 2 « Droit du commerce électronique et de l'économie numérique » proposé par l'Université Paris I Panthéon-Sorbonne (*http://www.m2droit-e-commerce.com/* [Consulté le 13 février 2018]).

30. Voir notamment la liste suivante des universités européennes dispensant des formations incluant la protection des données : Cambridge, Luxembourg, Leibniz Universitaet Hannover, Università degli Studi di Bologna, Strathclyde University Glasgow, Katholieke Universiteit Leuven, Queen Mary University of London, Université Notre-Dame de la Paix Namur, Universitetet i Oslo, Lapin yliopisto Rovaniemi, University of Vienna, Universidad de Zaragoza, Aristotle University Thessaloniki.

31. Voir à cet égard les lignes directrices du Groupe de travail Article 29 sur la protection des données (dit G29) sur le délégué à la protection des données, disponibles à l'adresse suivante : *https://www.cnil.fr/sites/default/files/atoms/files/guidelines_on_dpos_5_april_2017.pdf* [Consulté le 13 février 2018]. Le G29 préconise que le délégué possède les compétences suivantes : une expertise en matière de droit (national et européen) des données personnelles, une bonne compréhension des opérations de traitement effectuées par l'organisme qui l'a désigné, une bonne connaissance de cet organisme et de son secteur d'activité, la capacité de promouvoir une culture de la donnée au sein de cet organisme.

32. Article 38 s.3 du RGPD.

33. Au demeurant, le délégué n'est pas responsable en cas de non-respect du règlement. L'article 24.1 prévoit clairement que c'est le responsable du traitement ou le sous-traitant qui est tenu de « s'assurer et [d']être en mesure de démontrer que le traitement est effectué conformément » à ses dispositions. Le respect de la protection des données relève donc de la responsabilité du responsable du traitement ou du sous-traitant. Il n'est pas possible de transférer au délégué, par délégation de pouvoir, la responsabilité incombant au responsable de traitement ou les obligations propres du sous-traitant. En effet, cela reviendrait à conférer au délégué un pouvoir décisionnel sur la finalité et les moyens du traitement ce qui serait constitutif d'un conflit d'intérêts contraire à l'art.38.6 du RGPD.

34. La CNIL indique, à titre d'exemple, que les fonctions suivantes sont susceptibles de donner lieu à un conflit d'intérêts : secrétaire général, directeur général des services, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique, mais également d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. Un conflit d'intérêt peut également exister par exemple si un délégué, sur la base d'un contrat de services, représente l'organisme devant les tribunaux dans des dossiers impliquant des sujets en matière de données à caractère personnel.

35. Voir « Pénurie de DPO sur l'Europe, les entreprises face au RGPD européen », à l'adresse suivante : *http://itsocial.fr/enjeux-it/securite-dsi/cybersecurite/penurie-de-dpo-leurope-entreprises-face-rgpd-europeen/* [Consulté le 13 février 2018].

36. Voir, par exemple, « L'émergence des nouveaux métiers de la 'data' se heurte au manque de diplômés » à l'adresse suivante : *https://www.lesechos.fr/10/05/2016/LesEchos/22188-086-ECH_l-emergence-des-nouveaux-metiers-de-la—data—se-heurte-au-manque-de-diplomes.htm* [Consulté le 13 février 2018].

37. Voir l'art.37 s.2 du RGPD : « un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement ».

38. Voir par ex : *https://www.soluxions-magazine.com/externalisation-dpo-opportunite/* [Consulté le 13 février 2018].

39. Voir l'art.25 s.1 du RGPD : « le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ».
Si l'art.34 de la loi dite Informatique et Libertés prévoit déjà que « le responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès », l'art.25 du Règlement va au-delà et impose cette démarche proactive dans le but de répondre à toutes les exigences en lien avec la protection des données personnelles, sans la limiter à la seule obligation de sécurité.

40. « Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée » (art.25 s.2 du RGPD).

41. M. Dary & L. Benaissa, « *Privacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p.476.

42. M. Dary & L. Benaissa, « *Privacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p.476.

43. V.A. Cavoukian, « *Privacy by Design — The 7 foundational principles* », mai 2010 : *https://iapp.org/media/presentations/11Summit/RealitiesHO1.pdf* [Consulté le 13 février 2018].

44. M. Dary & L. Benaissa, « *Privacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p.476.

45. C. Zolynski, « La *Privacy by Design* appliquée aux Objets connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT*, 2016, p.404.

46. M. Griguer & J. Schwartz, « *Privacy by Design*/*Privacy by Default*. Une obligation de conformité et un avantage concurrentiel », *Cahiers de droit de l'entreprise*, no.3, mai 2017, prat.15.

47. M. Dary & L. Benaissa, « *Privacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p.476.

48. C. Zolinski, P. Pucheral, A. Rallet et F. Rochelandet, « La *Privacy by Design* : une fausse bonne solution aux problèmes de protection des données personnelles ? », Légipresse, no.340, juill.-août 2016.

49. Sur ce sujet, voir le rapport de l'*Information Commissioner's Office* intitulé « Big data, artificial intelligence, machine learning and data protection », disponible à l'adresse suivante : *https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf* [Consulté le 13 février 2018].

50. J. Verdure, « Le concept de « Privacy by Design » : un remède à l'insuffisance des moyens actuels de protection de la vie privée », févr. 2012, *http://www.e-juristes.org/le-concept-de-privacy-by-design-un-remede-a-linsuffisance-des-moyens-actuels-de-protection-de-la-vie-privee/* [Consulté le 13 février 2018].

51. Voir l'art.22, I de la loi dit Informatique et Libertés: « A l'exception de ceux qui relèvent des dispositions prévues aux arts 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés. »

