Réseau international d'avocats en droit du numérique et des technologies avancées
International lawyers' network for digital and emerging law

Le réseau Lexing® vous informe – The Lexing® network informs you

JTIT Internationale n° 18 –avril 2018
JTIT Special international issue #18– April 2018

MISE EN ŒUVRE DU RGPD : PRINCIPALES SPECIFICITES LOCALES

GDPR IMPLEMENTATION: MAIN LOCAL SPECIFICITIES

MISE EN ŒUVRE DU RGPD : PRINCIPALES SPECIFICITES LOCALES

▪ Le Règlement européen sur la protection des données (RGPD) est sous les feux de l'actualité. Ses dispositions seront directement applicables dans les Etats membres de l'Union européenne le 25 mai 2018. Autant dire demain.

▪ Si le RGPD est directement applicable, il nécessite néanmoins la révision des textes de loi nationaux afin d'abroger les dispositions incompatibles ou redondantes, d'adopter des dispositions nouvelles prévues par le RGPD, ou de prévoir des aménagements conformément à ses clauses dites « ouvertes » qui laisse une certaine marge de manœuvre laissée aux Etats membres.

▪ La France, la Belgique et les différents pays membres de l'UE sont sur les starting blocks. Les répercussions du RGPD dépasseront largement les frontières de l'Union européenne. Ce texte européen est d'ailleurs au cœur des débats devant le Congrès américain dans le cadre du scandale Cambridge Analytica.

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Australie, Belgique, France, Grèce, Mexique, Sénégal, Russie.

GDPR IMPLEMENTATION: MAIN LOCAL SPECIFICITIES

▪ *The European Data Protection Regulation (DGPR) is in the spotlight. Its provisions will be directly applicable in the EU Member States from 25 May 2018 onwards.*

▪ *Although the GDPR is directly applicable, it nevertheless requires the revision of national legislation in order to repeal incompatible or redundant provisions, to adopt new provisions provided for in the GDR, or to provide for adjustments in accordance with its so-called "open" clauses which leave a certain margin for manoeuvre left to the Member States.*

▪ *France, Belgium and the various EU member states are on the starting blocks. The GDPR has effects that will go far beyond the borders of the European Union. This European text is for example at the heart of the debates before the American Congress in the context of the Cambridge Analytica scandal.*

The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: Australia, Belgium, France, Greece, Mexico, Russia, Senegal, South Africa.

Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leur pays respectifs.

Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

https://lexing.network

AURELIE BANCK
Directeur du département
Conformité RGPD Banque et Assurance
du cabinet Lexing Alain Bensoussan-Avocats

Head of the GDPR Compliance for
Bank & Insurance department
of Lexing Alain Bensoussan-Avocats

Partout dans le monde, les entreprises se préparent avec effervescence à l'application imminente du règlement européen sur la protection des données, le fameux « RGPD ». Vu d'Afrique du Sud, le RGPD soulève trois grandes questions, au premier rang desquelles, bien entendu, la question de son applicabilité. Une fois qu'une entreprise sud-africaine a déterminé si elle doit ou non se conformer aux RGPD, deux autres questions essentielles suivent en cascade, concernant respectivement la désignation d'un délégué à la protection des données et d'un représentant dans l'UE.

Est-ce que je dois me conformer au RGPD ?

▪ La date butoir pour se conformer au RGPD étant fixée au 25 mai 2018, il est urgent de savoir si vous êtes concerné par ce texte et si vous devez vous y conformer.

▪ La question est d'importance car le champ d'application du RGPD est beaucoup plus large que de nombreuses entreprises ne le pensent. Le RGPD est en effet devenu *la* référence mondiale en matière de protection des données, et d'une certaine façon, l'Europe a exporté ses lois sur la protection des données dans le reste du monde.

▪ Pour déterminer si vous devez respecter ce texte ou non, vous devez vous poser cinq questions essentielles. Si vous répondez oui à au moins une des questions énoncées ci-dessous, alors vous entrez dans le champ du RGPD et devez par conséquent en respecter les dispositions :

- Etes-vous établi sur le territoire de l'UE ?
- Offrez-vous des biens ou des services aux citoyens de l'UE ?
- Suivez-vous le comportement de citoyens de l'UE ?
- Etes-vous le sous-traitant d'un responsable du traitement soumis au RGPD ?
- Avez-vous recours à un sous-traitant établi dans l'UE ?

Est-ce que je dois désigner un DPO ?

▪ ***Vous êtes un organisme public.*** Le RGPD dispose que tous les organismes publics (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle) doivent nommer un délégué à la protection des données (DPD), souvent désigné sous le sigle anglais « DPO » (data protection officer). Cependant, le RGPD ne définit pas ce qu'il entend par « organisme public ». Selon l'autorité britannique de protection des données, l'Information Commissioner's Office (ICO), en dehors des entités publiques et d'autres organismes qui n'existent manifestement qu'en tant qu'organismes publics, il appartiendra aux législations nationales des États membres de déterminer quels organismes privés seront également considérés comme des organismes publics au sens du RGPD.

▪ Ainsi, les organismes sud-africains devront vraisemblablement se référer aux dispositions des lois des États membres où se trouvent les personnes dont ils traitent les données à caractère personnel afin d'identifier clairement les organismes automatiquement considérés comme des organismes publics et ceux considérés comme tels uniquement lorsqu'ils remplissent certaines missions.

▪ ***Vos activités de base impliquent un traitement régulier ou un suivi régulier et systématique « à grande échelle ».*** Le RGPD impose aux responsables du traitement et aux sous-traitants dont les « activités de base » impliquent le traitement de catégories particulières de données à caractère personnel ou encore un « suivi régulier et systématique » des personnes concernées, « à grande échelle », de désigner un délégué à la protection des données.

▪ Ces différents concepts, qui restent assez flous pour les entreprises, ont fait l'objet de clarification dans des lignes directrices publiées par le groupe de travail européen sur la protection des données dit de l'« Article 29 » ou encore « G29 ». Pour ce dernier, les activités de base d'un organisme sont celles qui lui sont nécessaires pour atteindre ses principaux objectifs.

▪ Pour illustrer ces deux critères (« activité de base » et « régulier et systématique »), prenons l'exemple d'un hôpital : l'activité de base d'un hôpital est de fournir des soins de santé, et pour fournir des soins de santé, cet hôpital aura à collecter « régulièrement » et « conformément à un système », des données sur la santé. Autre exemple, celui d'une entreprise proposant des services d'externalisation RH. L'activité de base de cette entreprise consiste à réaliser des activités lui permettant de remplir efficacement les fonctions qui lui sont confiées par ses clients. Et dans le cadre de ces fonctions, l'entreprise va procéder au traitement permanent et systématique de données à caractère personnel.

▪ Enfin, s'agissant de l'expression « à grande échelle », le G29 reconnait la difficulté de la définir précisément, mais précise néanmoins qu'un traitement sera très probablement à grande échelle lorsqu'il concerne un nombre significatif de personnes concernées, sur une vaste zone géographique, et implique différents systèmes.

Est-ce que je dois désigner un représentant dans l'UE ?

▪ ***Le représentant dans l'UE*****.** Cette question intéresse bien entendu essentiellement les organismes qui ne sont pas établis sur le territoire de l'UE, car pour ceux établis dans l'UE, cette désignation n'est pas nécessaire puisque les personnes concernées et les autorités de contrôle peuvent les joindre facilement pour toute requête relative à la protection des données. Pour les organismes hors UE, donc, plusieurs facteurs sont à prendre en considération afin de déterminer s'ils sont dans l'obligation de désigner un représentant, et notamment : la nature des données à caractère personnel qu'ils traitent, si ce traitement comporte des risques pour les personnes concernées, ainsi que la quantité de données à caractère personnel traitée.

▪ ***Qui doit être ce représentant et dans quel pays doit-il être établi ?*** Le représentant est une personne, physique ou morale, à qui les personnes concernées et les autorités de contrôle de l'UE (en particulier celles des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement par l'organisme non établi dans l'UE) peuvent s'adresser facilement pour toutes les questions relatives au traitement mis en œuvre par l'organisme qu'il représente.

▪ Toutefois, le RGPD ne donne pas de détails sur qui peut être ce représentant et quelles sont les autres obligations qui lui incombent au titre de sa mission de représentation. Pas plus que sur son lieu d'établissement : faut-il désigner un représentant dans tous les Etats membre concernés par le traitement ? A cet

égard, le RGPD indique seulement, mais clairement, qu'un représentant doit être désigné et qu'il doit être établi dans au moins un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement.

▪ Il est intéressant de noter que le RGPD ne semble pas interdire à un DPD de remplir les fonctions de représentant. Le délégué à la protection des données d'un organisme pourrait donc très bien en être également le représentant, pour autant qu'il soit établi dans au moins un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement. Ce cumul de fonctions semble à première vue pratique dans la mesure où les tâches de ces deux rôles sont susceptibles de se recouper, mais il présente toutefois des inconvénients à prendre en considération. Si certaines des missions du DPD et du représentant se ressemblent, leurs fonctions sont, de fait, bien distinctes. En outre, il ne faut pas oublier que le RGPD impose spécifiquement certaines exigences relativement au DPD (et non au représentant), et notamment que le DPD fait directement rapport au niveau le plus élevé de la direction et qu'il ne peut être relevé de ses fonctions ou pénalisé par son organisme pour l'exercice de ses missions.

▪ ***Le représentant doit-il être indépendant et avoir des qualifications spécifiques ?*** Le représentant doit-il être un membre de l'entreprise ou bien est-il possible de choisir une personne indépendante externe à l'entreprise ? Doit-il être une personne légalement qualifiée ou s'apparente-il plutôt à un responsable des relations publiques ? Autant de questions pour lesquelles le RGPD reste silencieux. Le règlement européen se contente d'indiquer que le représentant doit communiquer sur les questions relatives à la protection des données de son organisme, tout en ne précisant pas ce que le représentant devrait savoir et les réponses qu'il est censé donner aux personnes concernées et aux autorités de contrôle en cas de violation des données, par exemple. Enfin, si le RGPD exige explicitement que le DPD soit indépendant, il n'est fait nulle mention du degré d'indépendance dont devrait jouir le représentant vis-à-vis de son organisme mandant.

▪ A cet égard, il est raisonnable de penser que la mission d'un représentant consiste à fournir des informations honnêtes aux personnes concernées et aux autorités de contrôle, avoir une connaissance suffisante des activités de traitement de l'organisme auquel il est rattaché afin de répondre a minima à des questions basiques, et à se référer au DPD pour les questions plus complexes.

▪ ***Quelle forme doit prendre cette désignation ?*** La désignation du représentant doit être faite par écrit. Cette exigence, posée par le RGPD, implique probablement que :

- la nomination du représentant se fasse par un contrat écrit ou par une lettre de nomination,
- l'organisme publie cette nomination sur son site Web, voire dans un message d'information adressé aux personnes concernées dont les données à caractère personnel font l'objet d'un traitement, et
- l'organisme transmette aux autorités de contrôle compétentes une communication écrite confirmant la nomination de ce représentant et indiquant ses coordonnées.

JOHN GILES

south-africa@lexing.network

▪ *Many organisations, both in South Africa and in other parts of the world, have started to implement the GDPR's requirements for data protection. In South Africa, there are three main issues that have surfaced during this implementation of the GDPR. The broadest question many of these organisations have asked is: Who must comply with the GDPR? Once they know that the GDPR applies to them and they have to comply with it, they usually raise the next two issues. One such issue is around the position of the Data Protection Officer (DPO), and the question: Who must appoint a DPO? Another question, which is connected in a way to the position of the DPO, is: Who must an organisation's representative be in the EU?*

Who must comply with the GDPR?

▪ *The deadline to comply with the General Data Protection Regulation (GDPR) is 25 May 2018. The big question is: Who must comply with it?*

▪ *Many people do not realise that this law has long tentacles and applies to many more organisations than they thought. It is the global gold standard for data protection. In some ways, Europe has exported their data protection laws to the rest of the world.*

▪ *In determining whether or not organisations have to comply, there are basically five questions people have to ask themselves. If they answer yes to any of the following questions, they have to comply with the GDPR.*

- *Are they established in the EU?*
- *Do they offer goods or services to people in the EU?*
- *Do they monitor the behaviour of people in the EU?*
- *Are they a processor for a controller who must comply?*
- *Do they have a processor in the EU?*

Who must appoint a DPO?

▪ ***Public bodies must appoint one*** *The GDPR says public bodies (except courts carrying out their normal judicial functions) have to appoint a DPO. The immediate issue that arises there is: What is a public body? The GDPR does not define a public body. The Information Commissioner's Office (ICO) suggests that apart from State-Owned Entities, and other bodies that clearly only exist as public bodies, it will be left to the national laws of Member States to determine what private bodies will also be deemed public bodies for the purposes of the GDPR.*

▪ *Based on this, South African organisations will probably have to look at what the laws of the Member States whose people they process personal data about, say. In other words, do those laws make it clear which organisations are always public bodies, and which are only public bodies when they serve certain functions?*

▪ ***Core activities involving regular processing on a large scale.*** *Organisations are struggling to understand what the GDPR means when it requires controllers*

and processors whose "core activities" involve processing special categories of personal data, for example, "on a large scale" to appoint DPOs. They are also struggling to understand what the GDPR means about processing that involves regular and systematic monitoring of data subjects on a "large scale". These organisations want to understand whether or not their processing activities fall within the ambit of that requirement.

▪ ***Regular and systematic monitoring of data subjects on a large scale.*** *The Article 29 Working Party, in providing guidance on these words, explains that core activities, firstly, are activities that an organisation wants to undertake in order to achieve its main goals.*

▪ *A hospital, for example, mainly aims to provide healthcare. When explaining the meaning of "regular and systematic monitoring," the Working Party, using the same hospital example, states that as a consequence of providing healthcare, the hospital will regularly, and in accordance with a system, collect health data. Another example to think of in explaining these words is an organisation that is the outsourced HR function for other organisations. This organisation's core activities will be activities that help it be an effective HR function for other organisations. As a consequence of being such a function, the organisation will continuously and systematically process personal data.*

▪ *For the words "on a large scale," the Working Party explains that while it is difficult to define these words exactly, the idea is that if the processing affects a significant number of data subjects, over a large geographical area, involving various systems, the processing is most likely happening on a large scale.*

Appointment of a representative in the EU

▪ ***Who must appoint a representative?*** *Many organisations need certainty about whether or not the GDPR requires them to appoint a representative. In asking this question, the organisations that are mostly in the dark are the ones that are not established in the EU. For the ones that are established in the EU the answer is a bit clearer – they do not have to appoint one, because they are established in the EU and data subjects and supervisory authorities generally have access to them regarding data-protection-related inquiries. For the organisations that are not established in the EU, there are various factors they have to consider in determining whether they have to appoint a representative or not. These factors include the nature of the personal data they process, whether such processing involves any risks to data subjects, the quantity of the personal data and various other considerations.*

▪ ***Who must the representative be?*** *The representative must be an accessible or contactable natural or legal person that data subjects and supervisory authorities in the EU (specifically the member states whose people the organisation is processing personal data about) can approach to inquire about the processing activities of the organisation they are representing.*

▪ *What is less clear, however, is who this person can be and what the other requirements around the role of this person are. One question about other requirements is: Does the representative have to have offices in the Member State whose people the organisation processes personal data relating to? The GDPR clearly states, in this regard, that an organisation only has to appoint a*

representative for at least one Member State.

▪ *What is quite interesting is that the GDPR does not seem to prevent a DPO from being the representative. An organisation's DPO might, therefore, very well be the representative, as long as they are based in at least one of the Member States whose people the organisation processes personal data relating to. This arrangement might work very well for organisations when considering that some of the functions of the two roles are slightly similar. There would, however, be possible disadvantages that organisations would carefully have to navigate their way around. This includes the fact that while the two roles are slightly similar, there are many differences. These differences include the DPO's direct reporting to an organisation's top management (who does the representative generally report to?), and the GDPR's provision that organisations may not dismiss DPOs on the basis of how they carry out their data-protection-related tasks.*

▪ ***Must the representative be independent and have qualifications?*** *When it comes to whether or not the representative should be someone from within the organisation or independent, a legally qualified person or someone akin to a Public Relations Officer, the GDPR is silent. What is clear from the GDPR is that the representative must communicate about their organisation's data protection matters. The GDPR is silent, however, on how much the representative would have to know and what answers they would have to give data subjects and supervisory authorities in the event of a data breach, for example. What is also not clear is the degree of independence the representative must have from their organisation. So far, the GDPR only explicitly requires the DPO to be independent from the organisation, not the representative.*

▪ *The safest conclusion to come to is that a representative should give honest information to data subjects and supervisory authorities, and have sufficient knowledge of the organisation's data processing activities in order to at least answer basic questions, while referring the more intricate questions to the DPO.*

▪ ***The appointment must be in writing.*** *Another requirement is that organisations must appoint or designate the representative in writing. This most likely involves three things:*

- *the representative must be appointed in terms of a written contract or a letter of appointment,*
- *the organisation must probably also publicise the appointment on its website, and perhaps even in a newsletter to the data subjects whose personal data the organisation processes, and*
- *the organisation must send relevant supervisory authorities a written communication confirming the appointment and supplying the contact details of the representative.*

JOHN GILES

south-africa@
lexing.network

▪ Avec la récente entrée en vigueur, en Australie, des lois sur les violations de données le 22 février 2018, les entreprises assujetties à la loi sur la protection données personnelles de 1988 ont déjà fort à faire. Un autre défi de conformité les attend pourtant déjà au tournant ! En effet, dès le 25 mai 2018, le règlement général sur la protection des données (RGPD) de l'Union européenne va s'appliquer et celui-ci concernera probablement de nombreuses entreprises australiennes qui sont « responsables » ou « sous-traitent » des traitements de données à caractère personnel dans l'UE.

▪ Le présent article présente le RGPD de manière synthétique et offre des conseils aux entreprises australiennes qui pourraient être concernées par sa prochaine application.

Le RGPD en bref

▪ Le RGPD est un règlement européen qui remplace la directive européenne de 1995 sur la protection des données (directive 95/46/CE) et vise à harmoniser les législations en matière de protection des données actuellement en vigueur dans les différents pays de l'UE.

▪ Les entreprises australiennes peuvent être tenues de se conformer au RGPD si :

- elles possèdent un établissement dans l'UE ;
- elles offrent des biens ou des services à des personnes qui se trouvent dans l'UE, ou suivent le comportement de ces personnes.

▪ Ainsi, une entreprise australienne ayant une présence physique dans l'UE sera soumise au RGPD, tout comme le sera une entreprise établie en Australie mais vendant sur son site Web des biens ou des services à des clients qui sont, eux, situés dans l'UE.

▪ De même, les entreprises nationales qui ne vendent pas nécessairement des biens ou des services, mais qui ont pour activité de référencer des clients ou des utilisateurs qui se trouvent dans l'UE ou de suivre le comportement de ces personnes, par exemple grâce à cookies ou des technologies similaires, entrent dans le champ d'application du RGPD.

Principaux changements introduits par le RGPD

▪ Les principales modifications apportées par le RGPD aux droits des personnes physiques ou des personnes concernées sont notamment les suivantes :

- Les personnes concernées ont le droit d'obtenir du responsable du traitement des informations sur la question de savoir si des données à caractère personnel les concernant sont traitées et si oui, à quelle fin ;
- Les personnes concernées ont un « droit à l'oubli », ce qui signifie qu'elles peuvent contraindre le responsable du traitement à effacer leurs données à caractère personnel, à cesser de toute diffusion de ces données et à demander aux tiers à qui ces données ont été communiquées de stopper leur traitement ;
- Les personnes concernées ont le droit de recevoir toutes les données à caractère personnel qu'elles ont fournies à un responsable du traitement ou à un sous-traitant dans un format structuré, couramment utilisé et lisible par machine, afin de les transmettre à un autre responsable du traitement ou à un autre sous-traitant.

Principales obligations à la charge des responsables du traitement

- Mettre en œuvre, dès la conception du système, des mesures techniques et organisationnelles appropriées et effectives en matière de protection des données ;
- Désigner un délégué à la protection des données qui fait rapport au niveau le plus élevé de la direction de l'entreprise et qui sera responsable de toutes les questions relatives à la protection des données ;
- Notifier les violations de données à caractère personnel :
  - Signaler ces violations à l'autorité de contrôle compétente dans les 72 heures ;
  - Lorsqu'une violation de données est susceptible d'engendrer un risque pour les droits et libertés des personnes, informer celles-ci dans les meilleurs délais ;
- Tenir un registre interne des violations de données ;
- Demander leur consentement aux personnes concernées sous une forme compréhensible et aisément accessible, en précisant la finalité du traitement ;
- S'interdire tout traitement de données sensibles, telles que des données concernant la santé, l'orientation sexuelle, la religion, les données génétiques, etc., à moins que la personne concernée n'ait donné son consentement explicite à ce traitement pour des finalités spécifiques ou que le traitement ne soit nécessaire en matière de droit du travail, de la sécurité sociale et de la protection sociale.

Sanctions en cas de non-conformité

▪ En Australie, la loi de 1988 sur la protection des données personnelles permet à l'autorité de protection des données, l'Information Commissioner, d'infliger des amendes pouvant atteindre 2,1 millions de dollars australiens pour les personnes morales et 420.000 dollars pour les personnes physiques. Ces sanctions semblent bien dérisoires en comparaison de celles introduites par le RGPD. En effet, en cas de violations du RGPD, les responsables du traitement ou les sous-traitants peuvent écoper d'amendes administratives pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu).

Plan d'actions

▪ Pour les entreprises australiennes susceptibles d'être soumises au RGPD, il n'y a plus de temps à perdre compte tenu des très nombreuses exigences et obligations à satisfaire. La tâche sera encore plus ardue en cas de traitement d'une grande quantité de données ou de catégories « particulières » de données sur le continent européen, la désignation d'un représentant établi sur le territoire de l'UE étant, dans ce cas, obligatoire.

▪ Il convient particulièrement de noter que l'obligation de signalement des violations de données introduite par le règlement européen impose d'effectuer ce signalement dans un délai de 72 heures, alors que les lois australiennes récemment entrées en vigueur accordent, quant à elles, un délai de 30 jours.

▪ Le RGPD instaure donc un certain nombre d'obligations en matière de conformité. Les entreprises australiennes concernées devront ainsi réfléchir et adopter une stratégie adéquate aux termes de laquelle elles choisiront soit de prendre les mesures nécessaires pour se conformer rapidement à ce texte, soit de réorganiser leurs activités afin de ne plus entrer dans le champ du RGPD et écarter ainsi le risque de sanctions. Quelle que soit la solution choisie, cette démarche nécessitera en tout état de cause de mettre en place une veille permettant de suivre l'évolution des obligations qui pourraient s'imposer à ces entreprises en Australie, en Europe et ailleurs dans le monde, et de manière générale, de mieux comprendre et appréhender les lois en matière de données à caractère personnel.

DUDLEY KNELLER

australia@lexing.network

▪ *With the introduction of Australian mandatory data breach laws on 22 February 2018, Australian businesses subject to the Privacy Act, 1988 are already having to quickly come to grips with this upcoming compliance obligation. However, another compliance challenge awaits! The EU General Data Protection Regulation (GDPR) commencing shortly thereafter, on 25 May 2018 will likely apply to many Australian businesses who "control" or "process" personal data in the EU.*

▪ *This paper briefly outlines the introduction of the GDPR and provides guidance for those Australian businesses which may be affected by its introduction.*

Some background on the GDPR

▪ *The GDPR replaces the existing 1995 Data Protection Directive (Directive 95/46/EC) and seeks to harmonise current data protection laws in place across the EU.*

▪ *Australian businesses may be required to comply with the GDPR if they:*

- *have an establishment in the EU;*
- *offer goods or services or monitor the behaviour of individuals in the EU.*

▪ *So clearly an Australian business with a physical presence in the EU will be captured, but so too will businesses operating out of Australia who use a website to sell goods or services to customers located in the EU.*

▪ *Even those businesses that do not necessarily sell goods or services but reference EU customers or users in the EU or track / monitor the behaviour of individuals using cookie or similar technologies will fall within scope.*

So what are the key changes in the GDPR?

▪ *Key changes to the rights of individuals or data subjects include the following:*

- *Data subjects are entitled to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed and for what purpose;*
- *Data subjects have the "right to be forgotten" which means that they can compel the data controller to erase their personal data, cease further dissemination of the data and have third parties halt processing of the data;*
- *Data subjects have the right to request and receive all personal data provided by them to a data controller or processer in a structured, commonly used and machine-readable format that can be provided to another data controller or processor.*

Key requirements or obligations for data controllers and processors

- *Implement appropriate and effective technical and organisational data protection controls from the onset of system design;*
- *Appoint a Data Protection Officer to report directly to the highest management level of the organisation and be responsible for all issues*

which relate to data protection;

- *Breach notification:*
  - *Report privacy breaches to the relevant supervisory authority within 72 hours.*
  - *Notify the individuals where a data breach is likely to result in a risk for the rights and freedoms of individuals, without undue delay;*
- *Keep internal register of any data breaches;*
- *Request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to the consent;*
- *Prohibition on processing of sensitive information such as health information, sexual orientation, genetic data, religion, etc. unless the individual has given express consent for a specified purpose or if processing is necessary in the context of employment, social security or social protection law.*

Penalties for non-compliance

▪ *Australian businesses are well aware of the increased powers of the Information Commissioner under the Privacy Act, 1988 with fines of up to $2.1 million for organisations and $420,000 for individuals. These penalties pale in comparison to those set to be introduced under the GDPR. Supervisory authorities will have the power to impose administrative fines for contraventions by controllers or processors, with fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher).*

Next steps

▪ *For those Australian businesses likely to be affected there is little time to waste with a raft of requirements and obligations which need to be met. A particular challenge arises for businesses which process large categories or "special" categories of data in the EU, with such organisations required to appoint an EU representative on the ground.*

▪ *Mandatory data breach obligations are also a little different with an obligation to report under GDPR within 72 hours as compared to the 30 day period soon to be imposed under the upcoming mandatory data breach laws in Australia.*

The GDPR presents a number of compliance hurdles and Australian businesses who are impacted will need to carefully assess whether they take the necessary steps to promptly comply or pare back their EU exposure whilst they consider their options moving forward in that region. Either choice nevertheless requires an increased understanding of the new laws and a strategy to keep pace with global compliance obligations as well as those affecting them in Australia.

DUDLEY KNELLER

australia@
lexing.network

Sous-traitants d'une autorité publique

▪ Le 3 décembre 2017, la loi portant création de l'autorité de protection des données a été adoptée par la Chambre des représentants. La Belgique a donc réformé son autorité de protection des données mais n'a pas encore publié le projet de loi de mise en œuvre du RGPD.

▪ Ce projet de loi est très attendu et les sous-traitants doivent rester attentifs d'une éventuelle obligation lorsqu'ils travaillent pour une autorité publique. On murmure en effet que les sous-traitants désignés par un responsable de traitement public devront disposer d'un délégué à la protection des données. Il n'est pas encore certain que cela s'appliquera à toutes les autorités ou seulement aux autorités fédérales, ni si cela aura une incidence sur les marchés publics en cours.

Loi du 3 décembre 2017 portant création de l'Autorité de protection des données

Recommandation n°04/2017 du 24 mai 2017

▪ La rumeur dit aussi que la Belgique abaissera l'âge de la majorité numérique à 13 ans.

Données relatives aux condamnations pénales et infractions

▪ Le RGPD (article 10) prévoit une protection spécifique en ce qui concerne les données concernant les condamnations pénales et les infractions ou les mesures de sécurité connexes. La directive 95/46 a laissé la possibilité aux États membres d'étendre ce statut spécial aux données relatives aux sanctions administratives ou aux jugements dans les affaires civiles. Le législateur belge a donc élargi la portée des données judiciaires aux affaires civiles.

▪ En opposition à la directive 95/46, le RGPD reste silencieux. Les données relatives aux litiges civils devraient donc être traitées comme des données personnelles régulières, à moins que la future législation belge ne prévoie une protection spécifique.

Conseiller en sécurité pour le système d'information

▪ Certaines législations belges spécifiques demandent déjà dans certaines hypothèses la nomination d'un conseiller en sécurité de l'information. Le conseiller en sécurité actuel, qui supervisait déjà les mesures de sécurité existantes, n'est peut-être pas la meilleure personne pour endosser le rôle de délégué à la protection des données. Il/elle deviendrait en effet juge de la conformité de sa propre politique de sécurité avec le RGPD.

▪ La Commission belge de la protection de la vie privée (qui s'appellera « Autorité de protection des données » à partir du 25 mai 2018) a adopté une recommandation qui donne des indications sur la compatibilité de la fonction de conseiller en sécurité avec la fonction de DPD, mais a délibérément choisi de ne pas fournir de réponse tranchée. La Commission de la protection de la vie privée conseille en effet au contrôleur et au sous-traitant d'examiner la compatibilité de ces fonctions au cas par cas et de garder une trace écrite de leur raisonnement.

FANNY COTON

belgium@lexing.network

Processors working for a public authority

▪ *On December 3rd, 2017, the law establishing the Data Protection Authority was adopted by the House of Representatives. Belgium has thus reformed its data protection authority but has not yet released the draft of GDPR implementation law.*

▪ *This draft law is much waited for, and processors should stay aware of a potential duty when contracting with a public authority. One murmurs that processors acting for a public controller should design a data protection officer. It is not yet certain if this will apply to all authorities or only to federal authorities, or if it will impact ongoing public procurements.*

▪ *The rumor also says that Belgium will lower the digital majority age to 13 years.*

Law of December 3rd, 2017 establishing the Data Protection Authority

Recommandation n° 04/2017 du 24 mai 2017

Data relating to criminal convictions and offences

▪ *GDPR (Article 10) provides for a specific protection regarding data relating criminal convictions and offences or related security measures. Directive 95/46 left the possibility for Member States to extend this special status to data relating to administrative sanctions or judgements in civil cases. The Belgian legislator had consequently widen the scope of judicial data to civil cases.*

▪ *In opposition to the Directive 95/46, the GDPR remains silent. Data relating to civil litigation should thus be treated as regular personal data, unless future Belgian law provides for a specific protection.*

Security Counsellor for the Information System

▪ *Specific Belgian legislations already ask in some hypothesis for the appointment of a Security Counsellor for the Information System. The existing Security Counsellor, who already supervised the existing security measures, may not be the best person to endorse the role of DPO. He/she would indeed become judge of the compliance of his/her own security policy with the GDPR.*

▪ *The Belgian Privacy Commission (to be called "Data Protection Authority from May 25th, 2018) has adopted a recommendation that gives some guidance on the compatibility of the function of Security Counsellor with the function of DPO, but has deliberately chosen not to provide a clear answer. The Privacy Commission advises the controller and the processor to examine the compatibility of these positions on a case by case basis and to keep written tracks of their reasoning*

FANNY COTON

belgium@lexing.network

Le régime administratif des formalités préalables

▪ Les entreprises françaises ou les organismes ayant la qualité de responsable du traitement ont l'habitude depuis 1978 et l'adoption de la loi du 6 janvier relative à l'informatique, aux fichiers et aux libertés (1) de déclarer auprès de la CNIL l'ensemble de leurs traitements de données à caractère personnel. En 2004, lors de la transposition de la Directive 95/46/CE en droit français, le législateur a soumis certains traitements de données comportant des données sensibles (comme des données biométriques ou le numéro de sécurité social ou ayant certaines finalités à une autorisation préalable de l'autorité de contrôle. Un traitement rentrant dans cette catégorie ne pouvait donc pas être mis en œuvre sans avoir reçu l'autorisation formelle de la CNIL, le silence de la Commission équivalent à un refus d'autorisation.

▪ Au fil des années la CNIL a adopté différents mécanismes de simplification afin de permettre d'alléger la charge inhérente à ces notifications préalables ; ces mesures prennent la forme d'un corpus de normes servant généralement de référentiels sectoriels ou thématiques à l'ensemble des entreprises. Ces normes publiques permettent également de diffuser la doctrine de la CNIL et de faire connaitre ses positions sur différents sujets (comme sur des durées de conservation ou les données que la CNIL considère comme pertinentes par rapport à une finalité donnée, etc.). Les consulter est devenu un réflexe pour tout professionnel de la protection des données exerçant en France.

Les changements induits par le RGPD

▪ Le règlement général sur la protection des données change ce paradigme. Il concrétise en effet un basculement d'un régime de formalité administrative à un régime de conformité globale visant à responsabiliser l'ensemble des acteurs de la chaine de traitement des données. La quasi-disparition des formalités préalables (2) à la mise en œuvre des traitements est perçue, en France, comme un allégement de la charge administrative pesant sur les entreprises. Elle n'est à n'en pas douter un facteur d'agilité. Il sera, en effet, plus simple d'enregistrer les traitements dans un registre tenu interne que de solliciter la CNIL voire patienter pendant plusieurs mois pour obtenir son autorisation. Elle génère cependant un risque et créé de l'incertitude.

▪ Un risque d'abord. Il faut bien l'avouer d'une manière générale les équipes projets ou les collaborateurs traitant des données personnelles étaient assez peu formés à la conformité Informatique et Libertés. La « Déclaration CNIL » était donc souvent un point d'entrée dans ce process et la matérialisation de ces exigences. Dès lors, la suppression de cette « déclaration » va nécessiter de mettre en place de nouveaux réflexes afin de s'assurer que le registre et les procédures seront effectivement alimentés et tenus à jour.

▪ Une incertitude ensuite. Les normes développées par la CNIL, ayant valeur réglementaire servaient de base à l'analyse de conformité et permettaient de déterminer avec une grande précision le régime juridique applicable à un traitement de données. Le règlement basé sur une approche par les risques modifie cette situation. Il implique, en effet, que chaque responsable de traitement effectue une analyse quant aux risques présentés par le traitement.

(1) Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

(2) Normes et dispenses de déclaration https://www.cnil.fr/fr/liste-des-normes-et-des-dispenses

(3) Projet de loi français d'application au RGPD: http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp

On passe donc d'un régime objectif à un régime où chaque acteur devra lui-même procéder à l'appréciation des risques présentés par une opération de traitement. Son appétence, sa sensibilité aux risques tout comme sa connaissance des règles de protection des données seront donc déterminantes.

▪ Enfin, il faut noter que la documentation des traitements, des processus et procédures mises en place pourrait s'avérer plus lourd que la simple déclaration des traitements auprès de la CNIL. En effet, l'obligation d'Accountability n'oblige pas simplement à documenter les traitements mais à apporter la preuve de la conformité aux dispositions du règlement, ce qui au final s'avère beaucoup plus complexe. Complexité renforcée par la dimension temporelle. En effet, si la déclaration auprès de la CNIL était relativement statique, les mesures mises en place au titre de l'Accountability seront à m'en pas douter dynamique pour s'adapter aux contextes changeant dans lesquels les traitements de données sont mis en œuvre. C'est donc à un changement culturel que la France doit faire face.

Une solution : la conduite du changement

▪ Au-delà de la technicité du projet de mise en conformité, il apparait fondamentale en particulier en France d'accompagner les changements au sein des organisations. Le vrai défi de l'Accountability réside en effet, dans le maintien en condition opérationnelle de l'ensemble des outils qui seront mis en place dans le cadre du projet de mise en conformité. Et c'est ce maintien qui garantira la conformité de l'organisme de manière pérenne et qui le plus à même d'éviter les non-conformités.

▪ Cette conduite du changement passe par la sensibilisation et la formation de l'ensemble des personnels de l'entreprise en particulier des chefs de projet (assistance à maitrise d'ouvrage et à maitrise d'œuvre) qui ont vocation à accompagner les business lines dans leurs nouveaux projets. Elle passe aussi par un engagement fort de la Direction au plus haut niveau et une responsabilisation des équipes opérationnelles, qui traitent leurs données, les équipes support se limitant à une fonction d'assistance à la mise en conformité. Enfin, le DPO en tant que chef d'orchestre devra maintenir cette culture dans le temps et s'assurer à l'aide de différents outils (formation, communication, etc.) que le réflexe « Informatique et Libertés » est ancré dans chaque collaborateur.

Et les référentiels de la CNIL ?

▪ Le corpus de normes adoptées par la CNIL n'a, cependant, pas vocation à disparaitre. Le projet de loi français (3) visant à adopter certaines spécificités locales prévues par le règlement prévoit en effet que la CNIL pourra adopter « des référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants ».

▪ Accountability et responsabilisation des acteurs mais la CNIL a vocation à continuer la diffusion de bonnes pratiques, la questions suivante étant quelle sera la valeur normative de ces référentiels ?

AURELIE BANCK
france
@lexing.network

The burden of administrative formalities and the cutting of red tape

▪ *Since 1978 and the adoption of Data Protection Act (1), French organisations with the status of data controller have been required to notify all their personal data processing to the national data protection authority, the CNIL. Moreover, in 2004, when transposing Directive 95/46/EC into French law, the legislator made some categories of processing involving sensitive data (such as biometric data or social security numbers) subject to prior authorisation by the CNIL. A processing operation falling into those categories could not therefore be implemented without having first received formal authorisation from the CNIL; the Commission's silence amounted to a refusal of authorisation.*

▪ *Over the years, the CNIL adopted various simplification measures in order to lighten the burden associated with those prior notifications and cut red tape; these measures together form a body of standards generally serving as sector-specific or thematic reference documents for all companies. These public standards also make it possible to disseminate the CNIL's doctrine and publicize its positions on various subjects (such as retention periods or data that the CNIL considers relevant to a given purpose, etc.). Consulting them is a must for any data protection expert working in France.*

Changes brought about by the GDPR

▪ *The General Data Protection Regulation changes this paradigm. It embodies a shift from an administrative formality regime to a global compliance regime aimed at empowering all actors in the data processing chain. The virtual disappearance of the formalities to be taken (2) prior to data processing is perceived in France as a reduction of the administrative burden on businesses. It is undoubtedly a factor of agility. It will indeed be easier to register the processing operations in an internal record than asking the CNIL to do so or waiting several months to obtain its authorisation. This will create risk and uncertainty, though.*

▪ *A risk first. It is necessary to admit that the project teams or the various stakeholders processing personal data are generally poorly trained on data protection compliance. The "CNIL notification" was often therefore a reality, check, a first step on the road of compliance; a way to give form to data protection and grasp its requirements. Therefore, the impending removal of the CNIL notification will require new reflexes to be acquired in order to ensure that the data records and procedures will be effectively maintained and kept up to date.*

▪ *Uncertainty, then. The standards developed by the CNIL, having regulatory value, served as the basis when performing a compliance analysis and made it possible to determine with great precision the legal regime applicable to a specific data processing operation. The GDPR, which introduces a risk-based approach, changes the rules of the game. It implies that each controller carries out an analysis of the risks presented by the processing. We are therefore moving from an objective system to a system where each player will have to assess the risks presented by a processing operation themselves. That player's data protection culture (including knowledge of the data protection risks and*

(1) Data Protection Act of 6 January 1978: https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

(2) Standards and Reporting Exemptions https://www.cnil.fr/fr/liste-des-normes-et-des-dispenses

(3) French GDPR Implementation Bill : http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp

rules) will therefore be decisive.

▪ *It should also be noted that the documentation, processes and procedures put in place by the GDPR in respect of the processing could turn out to be more cumbersome than the CNIL notification. The Accountability requirement introduced by the GDPR does not simply require to document the processing operations, but also to be able to demonstrate compliance with the EU Regulation — which at the end of the day proves to be much more complex. A complexity reinforced the time factor: while the CNIL notification was relatively static, the measures put in place under Accountability will undoubtedly be dynamic to adapt to the ever-changing contexts in which data processing is implemented. A real cultural change is thus needed in France.*

A solution: change management

▪ *Beyond the technical nature of the compliance project, it seems fundamental, particularly in France, to support change within organizations. The real challenge of accountability lies in maintaining in operational condition all the tools that will be put in place as part of the compliance project. This will be instrumental in guaranteeing the sustainability of organisation's compliance and in avoiding non-compliances.*

▪ *This change management involves raising awareness and training all company personnel, in particular project managers (project management and project management assistance), who are responsible for supporting business lines in their new projects. It also requires strong commitment at the highest level of the company and accountability of the operational teams who process the data, with support teams limited to a compliance assistance function. In this respect, the DPO will act as a true leader in maintaining this culture over time and ensure, with the help of various tools (training, communication, etc.), that the data protection is anchored in each employee.*

What about the CNIL's standards?

▪ *Be that as it may, the body of standards adopted by the CNIL is not intended to disappear. The French GDPR Implementation Bill (3) aimed at adopting certain local specificities provided for by the EU Regulation provides that the CNIL may adopt "standards designed to facilitate the compliance of personal data processing with texts relating to the protection of personal data and to carry out prior risk assessment by data controllers and their processors".*

▪ *Accountability is a key principle of the GDPR and requires all stakeholders to be responsible and accountable for their processing of personal data; but one of the CNIL's tasks is and will continue to be the development of good practices and standards. The big question is, what will be the normative value of these standards?*

AURELIE BANCK
france
@lexing.network

Une échéance qui se rapproche

▪ Après un délai de grâce de deux ans suivant son adoption, le règlement général sur la protection des données (RGPD) deviendra bientôt directement applicable dans l'ensemble des pays de l'Union européenne, le 25 mai 2018. Pourtant, alors que cette date butoir approche, de récents sondages **(1)** démontrent qu'en dépit des lourdes sanctions encourues en cas de non-respect des dispositions de ce texte, plus d'une organisation européenne sur quatre estiment qu'elles ne seront pas prêtes à temps.

La marge de manœuvre laissée aux Etats membres par les clauses dites ouvertes

▪ Certaines clauses du RGPD laissent aux États membres une marge de manœuvre leur permettant d'ajuster les règles posées par ce texte européen à leur situation nationale. Il s'agit par exemple des clauses concernant le traitement de données dans le cadre des relations de travail, ou encore la désignation du délégué à la protection des données. Une commission législative a bien été instituée en Grèce afin de plancher sur ce sujet, mais pour le moment aucun projet (officiel ou non) de texte n'a été publié, divulgué ou débattu publiquement. Le RGPD contient 70 clauses ouvertes, et l'harmonisation du droit de la protection des données souhaitée par le législateur européen et, par ricochet, l'efficacité du mécanisme de guichet unique instauré par le RGPD dépendra ainsi grandement de la manière dont la Grèce et les autres Etats membres décideront d'exercer leur droit d'introduire une législation nationale parallèle par le biais de ces clauses.

La portabilité des données

▪ L'expression « portabilité des données » désigne le droit accordé, dans certains cas, aux personnes concernées, de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de transmettre ces données à un autre responsable du traitement. Déja controversée lors du processus de négociation de RGPD, la portabilité des données risque bien de rester une question sensible. Initialement destinée à s'appliquer aux fournisseurs de services de médias sociaux, voire aux fournisseurs de services de télécommunications, la terminologie finalement adoptée par l'article 20 du RGPD a considérablement élargi sa portée, comme en témoigne le considérant 68 du RGPD, aux termes duquel « Il y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données ». Ce droit nécessitera donc forcément des entreprises un effort d'investissement en ce sens. A noter que le groupe travail « Article 29 » a publié des lignes directrices sur le droit à la portabilité des données **(2)**.

(1) "Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation", IAPP - TrustArc, novembre 2017, disponible à l'adresse : https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf

(2) « Lignes directrices relatives au droit à la portabilité des données », Groupe de travail « Article 29 », adoptées le 13 décembre 2016, et révisées le 5 avril 2017, disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf

L'agenda bien rempli des autorités de protection des données

▪ Alors même que le RGPD supprime certaines des formalités préalables (déclarations, autorisations) à accomplir auprès de l'autorité de protection des données, il semble peu probable que cette suppression allège la charge de travail déjà bien lourde de l'autorité grecque, en sous-effectif. Bien au contraire, les autorités de contrôle nationales se voient confier de nouvelles missions par le RGPD, telles que l'obligation d'agir ou d'apporter leur assistance en matière d'analyses d'impact ou de violation de données. Reste donc à voir si, dans la pratique, ces nouvelles missions affecteront la capacité de surveillance et l'efficacité de l'autorité grecque.

La conformité : à quel prix ?

▪ Selon des études récentes **(1)**, plus d'un professionnel de la protection de la vie privée sur quatre dans l'UE affirme que son organisme ne sera pas prête en temps et en heure pour l'application du RGPD. Le principal obstacle se dressant sur le chemin de la conformité semble tenir à l'absence de budget adéquat. Si le coût d'une mise en conformité efficace (le montant est variable en fonction de la taille de l'organisme, du secteur concerné et de la nature des traitements des données opérés) peut certes être élevé, on peut légitimement rétorquer que ce coût serait nettement inférieur à celui des sanctions auxquelles ce même organisme s'exposerait en cas de non-conformité. Les données sont des actifs commerciaux précieux et une non-conformité peut engendrer des conséquences aussi multiples que variées : sanctions administratives, actions en responsabilité, atteinte à la réputation et à l'image de marque, perte de revenus, etc.

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

The countdown

▪ *On May 25, 2018, following a 2 year post-adoption grace period, the General Data Protection Regulation (GDPR) will become fully enforceable throughout the European Union. Today, despite the severe sanctions envisaged by the GDPR for non-compliance, based on recent surveys **(1)**, it appears that more than one in four EU organizations don't have confidence they'll be in full compliance.*

Opening clauses

▪ *Certain GDPR rules allow Member States to introduce national provisions to adapt the application of the rules of the GDPR, e.g. with regard to data processing in the context of employment, the appointment of a data protection officer, etc. A relevant legislative committee has been set up in Greece, but for the time being no (official or unofficial) draft has been published, leaked or publicly discussed. The fact that the GDPR contains 70 opening clauses and the degree that the Greek state and other Member States will decide to exercise their right to introduce parallel national legislation, will essentially determine the degree of harmonization of data protection laws throughout Europe and, at the end of the day, how effectively the GDPR one-stop-shop principle will apply.*

Data portability

▪ *Data portability is the data subject's right, under certain circumstances, to receive his/her personal data, which s/he has provided to a controller, in a structured, commonly used and machine-readable format and the right to transmit those data to another controller. Data portability has been, during the GDPR negotiation process, a controversial issue, and we expect to remain so. While, as it seems, original intention was to primarily regulate social media service providers and probably also telecom service providers, language finally adopted in GDPR article 20 has substantially broadened the applicability scope. In fact, according to GDPR recital (68), "data controllers should be encouraged to develop interoperable formats that enable data portability", which for businesses will necessarily require a relevant investment. Guidelines on the right to data portability have been published by the WP29 **(2)**.*

DPA workload

▪ *Despite the fact that, under the GDPR, requirements to submit notifications to and obtain approvals by the Greek Data Protection Authority (DPA) about certain data processing activities will be abolished, it seems likely that, nevertheless, the currently heavy workload of the (understaffed) DPA will not improve. Quite the contrary; there are instances under the GDPR when the DPA will need to take action and offer assistance, e.g. for the needs of privacy impact assessments and in the case of data breaches. It remains to be seen in practice, whether the DPA's new roles and duties will affect its monitoring ability and efficiency.*

(1) "*Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation*", IAPP - TrustArc, November 2017, available at https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf

(2) "Guidelines on the right to data portability" adopted on 13 December 2016, Article 29 Working Party, available at http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Cost of compliance

▪ *According to recent surveys **(1)**, more than one in four EU privacy professionals say their organisations will not be ready on time, with the biggest barrier apparently being the lack of adequate budget. While, indeed, the cost of effective compliance can (depending on the size of the organisation, the industry and the nature of data processing) be high, it can be validly argued, that the said cost would be far less that the cost of non-compliance. Notably, data are valuable business assets and non-compliance could have multiple consequences for organisations: administrative sanctions, liability for damages, reputational damage, revenue loss, etc.*

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@
lexing.network

Qu'est-ce que RGPD ?

▪ Le RGPD est le sigle désignant le règlement général sur la protection des données, qui entrera pleinement en application à compter de mai 2018. Bien qu'il s'agisse d'un instrument juridique européen, les dispositions du RGPD auront une incidence à l'échelle mondiale, Mexique y compris, dans la mesure où leur champ d'application couvre toutes les données à caractère personnel des citoyens de l'UE.

Loi mexicaine sur la protection des données vs. RGPD

▪ Le cadre légal mexicain en matière de protection des données est constitué de la loi fédérale sur la protection des données personnelles détenues par des parties privées, de ses règlements d'application et des résolutions prises par l'autorité mexicaine de protection des données (INAI) **(1)**. Promulgué en 2010, la loi fédérale s'inspire des lois européennes et américaines, ainsi que des principes de l'APEC en matière de données à caractère personnel.

▪ La loi et ses règlements consacrent plusieurs principes de protection des données à caractère personnel, qui s'appuient sur les concepts de légalité, de consentement, d'avis de confidentialité (« aviso de privacidad »), de qualité, de finalité, de fidélité, de proportionnalité et de responsabilité (« accountability »).

▪ En résumé, ces principes exigent que les responsables du traitement des données, les sous-traitants et autres intervenants se conforment à des normes minimales de protection des données, et notamment par l'aménagement adéquat de la relation juridique existant entre le responsable du traitement et les sous-traitants, par la bonne gestion des traitements des données dans le Cloud, et par la mise en œuvre des meilleures pratiques et de technologies propres à protéger ces données contre les vulnérabilités et les cyber-attaques.

▪ Par certains aspects, les dispositions mexicaines présentent des similitudes avec celles du RGPD. C'est le cas notamment en matière de responsabilité **(2)** et de gouvernance des données, d'analyses d'impact **(3)**, de mesures de sécurité **(4)** et de protection des données dès la conception, de désignation d'un responsable (« CPO ») ou d'un service en charge de la protection de la vie privée au sein des entités qui traitent les données **(5)**, de droit à l'oubli **(6)** et d'auto-évaluation et de certification en matière de protection des données **(7)**. Sur ce dernier point, on peut noter qu'avant la promulgation de la loi fédérale sur la protection des données en 2010, il existait un système d'auto-certification : les entreprises mexicaines pouvaient obtenir auprès de l'Association mexicaine pour l'Internet un certificat attestant de leur conformité aux principes de l'APEC.

▪ Toutefois, les législations du Mexique et de l'UE diffèrent sur plusieurs points, et notamment sur la notion d'« intérêt légitime », posée comme une des conditions de licéité du traitement des données par le RGPD, contrairement à la loi mexicaine. En revanche, la loi mexicaine accepte, quant à elle, le consentement tacite, excepté lorsque sont en jeu des données personnelles sensibles, entendu comme les données concernant la vie d'une personne, les données dont l'utilisation abusive peut conduire à une discrimination ou impliquer un risque grave pour la personne concernée, ou encore les données qui révèlent l'origine raciale ou ethnique, l'état de santé actuel et futur, les convictions religieuses, philosophiques et morales, l'appartenance syndicale, les opinions politiques, la préférence sexuelle, les

REFERENCES

(1) L'INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) est une entité publique constitutionnelle et autonome qui garantit le droit d'accès des individus aux informations publiques gouvernementales, protège les données personnelles détenues par le gouvernement fédéral et les individus et se prononce sur les aspects négatifs de l'accès aux informations des entités publiques fédérales.

(2) Le principe mexicain de responsabilité, aujourd'hui également énoncé par le RGPD, renvoie à l'obligation du responsable du traitement de se conformer aux dispositions applicables sur les mesures de protection des données à caractère personnel par des mesures techniques et organisationnelles appropriées au regard des risques.

(3) Article 48 du Règlement d'application de la Loi fédérale sur la protection des données à caractère personnel détenues par des parties privées.

(4) Article 19 de la loi de 2010

(5) Article 30 de la loi de la loi de 2010

(6) La première affaire concernant le « droit à l'oubli » au Mexique concernait la demande de adressée par un entrepreneur mexicain qui a demandé à la société Google Mexico, S. de R. L. de C. V. aux fins de déréférencer des contenus portant atteinte à sa réputation. La décision rendue par l'INAI est consultable à l'adresse

données génétiques etc.).

▪ Enfin, les textes mexicains possèdent leurs spécificités propres, notamment en ce qui concerne la mention d'information **(8)**, la formation à dispenser régulièrement aux dirigeants et aux salariés en matière de protection des données, les modalités d'exercice des droits dits « ARCO » **(9)**, le flux des données, les formats pour la collecte de données, les relations entre les responsables du traitement **(10)** et les sous-traitants **(11)**, etc. Tout manquement est assorti de lourdes amendes.

▪ **Structure de la loi mexicaine.** La loi sur la protection des données s'articule autour des chapitres suivants : i) Dispositions générales, ii) Principes de protection des données à caractère personnel, iii) Droits des propriétaires de données, iv) Exercice des droits d'accès, de rectification, d'annulation et d'opposition, v) Transfert de données, vi) Autorités, vii) Procédure de protection des droits, viii) Procédure de vérification, ix) Procédure d'application de pénalité et x) Dispositions transitoires.

▪ **Champ d'application territorial**. Le champ d'application territorial de la loi mexicaine sur la protection des données est posé à l' article 4 de son règlmeent d'application :

> ***Champ d'application territorial***
>
> *Article 4. Le présent règlement s'applique obligatoirement à tout traitement lorsque :*
>
> *Il est effectué dans un établissement du responsable du traitement établi sur le territoire mexicain ;*
>
> *Il est effectué par un sous-traitant, quel que soit le lieu où il se trouve, pour le compte d'un responsable du traitement établi sur le territoire mexicain ;*
>
> *Le responsable du traitement des données n'est pas établi sur le territoire mexicain, mais est soumis aux lois mexicaines en vertu de la conclusion d'un contrat ou en vertu du droit international ; et*
>
> *IV. Le responsable du traitement n'est pas établi sur le territoire mexicain mais utilise des moyens sur ledit territoire, à moins que ces moyens ne soient utilisés uniquement à des fins de transit qui n'impliquent pas un traitement. Aux fins du présent paragraphe, le responsable du traitement fournit les moyens nécessaires à l'accomplissement effectif des obligations imposées par la loi, son règlement d'application et les autres dispositions applicables, découlant du traitement des données à caractère personnel. A cette fin, il peut désigner un représentant ou mettre en œuvre le mécanisme qu'il juge pertinent, à condition que le responsable du traitement soit en mesure de respecter effectivement, sur le territoire mexicain, les obligations que la réglementation applicable impose aux entités qui traitent des données personnelles au Mexique.*
>
> *Lorsque le responsable du traitement n'est pas établi sur le territoire mexicain, mais que le sous-traitant l'est, ce dernier est soumis aux dispositions relatives aux mesures de sécurité prévues au chapitre III du présent règlement.*
>
> *S'agissant des personnes physiques, on entend par établissement le lieu où se trouve le siège principal de leur entreprise, ou celui qu'elles utilisent pour l'exercice de leurs activités, ou leur domicile.*
>
> *S'agissant des personnes morales, on entend par établissement le lieu où se trouve l'administration principale de l'entreprise et, pour les personnes morales situées à l'étranger, le lieu où se situe l'administration principale de cette personne sur le territoire mexicain, ou, à défaut, tout lieu désigné par elles, ou toute installation stable qui permet l'exercice effectif ou réel d'une activité. »*

▪ Tout comme le RGPD, les dispositions du cadre juridique mexicain sur la protection des données peuvent, par conséquent être extraterritoriales. En outre, l'article 36 de la loi fait référence aux transferts à des tiers autres que les responsables du traitement :

> *« Article 36. Lorsque le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers des tiers nationaux ou étrangers autres que le responsable du traitement, il doit leur communiquer l'avis relatif au respect de la vie privée et les finalités*

suivante : http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf

(7) L'autorégulation est posé à l'article 44 de la loi de 2010 « Article 44. Les personnes physiques ou morales peuvent conclure des accords entre elles et avec des organisations civiles ou gouvernementales nationales ou étrangères sur les mécanismes d'autorégulation en la matière, qui complètent les dispositions de la présente loi. Ces systèmes doivent comprendre des mécanismes permettant de mesurer leur efficacité en matière de protection des données, les conséquences et les mesures correctives efficaces en cas de non-respect. Les systèmes d'autorégulation peuvent se traduire par des codes d'éthique ou de bonne pratique professionnelle, des sceaux de confiance ou d'autres mécanismes, et comporteront des règles ou normes spécifiques permettant d'harmoniser le traitement des données effectué par les adhérents et de faciliter l'exercice des droits des titulaires de données. Ces régimes seront notifiés simultanément aux autorités sectorielles compétentes et à l'Institut.

(8) Article 16 de la loi de 2010 : « L'avis de confidentialité doit contenir au moins les informations suivantes : I. L'identité et le domicile du responsable du traitement qui collecte les données ; II. Les finalités du traitement des données ; III. Les options et les moyens offerts par le responsable du traitement aux propriétaires des données pour limiter l'utilisation ou la divulgation des données ; IV. Les moyens d'exercer les droits d'accès, de rectification, d'annulation ou d'opposition,

pour lesquelles le propriétaire des données a accepté le traitement de ses données. Le traitement des données doit être réalisé conformément à l'avis relatif au respect de la vie privée, qui contient une clause indiquant si la personne concernée accepte ou non le transfert de ses données ; en outre, le tiers destinataire assumera les mêmes obligations que le responsable du traitement des données qui lui a transféré les données ».

▪ Enfin, le Mexique a récemment été invité à adhérer à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n°108) du Conseil européen et à son protocole additionnel.

En résumé : les points à retenir

▪ Dans de nombreux pays du monde, les entreprises vont devoir prendre des mesures afin de se conformer au RGPD, qui s'applique au traitement de données à caractère personnel de personnes physiques de l'UE.

▪ Pour ce qui concerne plus particulièrement le Mexique, la mise en conformité au RGPD nécessitera de :

- Respecter les mesures techniques et organisationnelles, notamment, en ce qui concerne :
  - la cartographie des données personnelles,
  - la durée de conservation des données,
  - la pseudonymisation et le chiffrement des données,
  - la portabilité des données,
  - l'obligation de signaler les violations de données et la mise en place de plans et dispositifs associés,
  - la réalisation d'une analyse d'impact en vue de réduire les atteintes aux droits et libertés des personnes,
  - la mise en place de mécanismes permettant d'être en mesure de prouver que le traitement a obtenu le consentement des personnes concernées et est nécessaire aux fins d'intérêts légitimes,
  - auditer et, le cas échéant, renégocier les contrats conclus avec les fournisseurs ayant accès aux données à caractère personnel,
  - vérifier les transferts de données effectués au niveau national et international, etc. ;
- Modifier les missions incombant au responsable ou au service en charge de la protection de la vie privée afin d'y intégrer les tâches nécessaires au respect du RGPD ; et
- Mettre à jour la gouvernance d'entreprise afin de s'assurer que l'entreprise est en conformité avec le RGPD et que les collaborateurs bénéficient de formations actualisées.

conformément aux dispositions de la présente loi ; V. Le cas échéant, les transferts de données à effectuer, et VI. La procédure et les moyens par lesquels le responsable du traitement informera les propriétaires des données des modifications apportées à l'avis de confidentialité, conformément aux dispositions de la présente loi. Pour les données personnelles sensibles, l'avis de confidentialité doit indiquer expressément qu'il s'agit de ce type de données. »

(9) ARCO est un acronyme utilisé au Mexique et en Espagne pour désigner les droits d'accès, de rectification, d'annulation et d'opposition dont bénéficient grâce à la loi les personnes à l'égard de leurs données à caractère personnel (Derechos ARCO: Acceso, Rectificación, Cancelación, Oposición).

(10) Article 15 de la loi de 2010

(11) L'article 3, paragraphe IX de la loi de 2010définit le « la personne physique ou morale qui, seule ou conjointement avec d'autres, traite des données à caractère personnel pour le compte du responsable du traitement. »

ENRIQUE OCHOA
DE GONZÄLEZ ARGÜELLES

mexico@
lexing.network

What is GDPR?

▪ *The General Data Protection Regulation (GDPR) will enter into full force and effect as of May, 2018. These provisions –although a European legal instrument- will impact worldwide since their scope refers to personal data of EU citizens and its processing and non-compliance of said provisions may lead to large fines.*

Mexican legal framework on data protection and GDPR

▪ *Mexican legal framework on data protection includes the Federal Data Protection Law Held by Private Parties, its Regulations and other provisions by the Mexican Data Protection Agency (INAI) **(1)**. Said legal framework was enacted in 2010 and has influence from the European and American Laws, as well as APEC Principles.*

▪ *The Law and the Rules refer, among others to the Principles of Personal Data Protection which are: legality, consent, notice, quality, purpose, fidelity, proportionality and accountability.*

▪ *In a nutshell, these Principles require the Data Controllers, Data Processor and others to comply with minimum standards of data protection including the legal relation between Data Controller and Data Processors, the treatment of data in cloud computing, as well as for the entities involved in the treatment of personal data to have the best practices and technology in order to protect said data from vulnerabilities and cyber-attacks.*

▪ *There are also several similarities with the GDPR concerning accountability **(2)** and data governance, Data Protection Impact Assessment **(3)** (DPIA), security measures **(4)** and "Privacy by Design", the appointment of a Chief Privacy Officer (CPO) or Department within entities which process data **(5)**, right to be forgotten **(6)**, and self-regulation and certification on data protection **(7)**. As concerns self-regulation, before the enactment of the data protection legal framework Mexico had a self-regulation certification by the Mexican Internet Association which made possible for entities to comply with APEC Principles and to have a certification thereof.*

▪ *One of the biggest differences between the Mexican legal framework and GDPR is the concept of "legitimate interest for the processing of personal data". Mexican legal provisions refer to tacit consent, but sensitive personal data such as: individual´s life or whose misuse might lead to discrimination or involve a serious risk for the data holder, which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, sexual preference, etc., and GDPR specifically requires said legitimate interest.*

REFERENCES

(1) INAI is the acronym for Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, which is a constitutional and autonomous public entity which guarantees the rights of access for individuals to governmental public information, protects personal data in hands of both the federal government and individuals and resolves on the negatives of access to the information of federal public entities.

(2) Nowadays a Principle referred to in the GDPR. This Principle refers to the obligation of the Data Controller to comply with applicable provisions on measures to protect personal data by technical and organizational measures on relevant risks.

(3) As concerns the Principle of Accountability, article 48 of the Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties

(4) Article 19 of the Law,

(5) Article 30 of the Law.

(6) The first case regarding the "right to be forgotten" in Mexico was based on a claim by a Mexican entrepreneur who asked GOOGLE MEXICO, S. DE R.L. DE C.V. the removal of indexed content that harmed his reputation. The Decision by INAI is available at http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf

(7) Article 44 of the Law

(8) Article 16 of the Law refers to the Privacy Notice as follows: "Article 16. The privacy notice must contain at

▪ *On the other hand, Mexican provisions are unique and enforceable concerning, among others: the "Privacy Notice" **(8)**, the periodical training for officers and employees regarding data protection, the procedures for ARCO **(9)** actions, flow of the data, formats for the collection of said data, the interaction and operation between Data Controllers **(10)** and Data Processors **(11)**, etc. In line with the above, fines in such legal framework are large and expensive.*

▪ *For easy reference, the Law is divided in the following chapters: i) General Provisions, ii) Principles of Personal Data Protection, iii) Rights of Data Owners, iv) Exercise of Rights of Access, Rectification, Cancellation and Objection, v) Data Transfer, vi) Authorities, vii) Rights Protection Procedure, viii) Verification Procedure, ix) Penalty Application Procedure and x) Transitory Provisions.*

▪ *Furthermore, the scope of territorial application of Mexican legal framework is as follows. The Rules of the Law set forth in Article 4 that:*

> ***Territorial scope of application***
>
> *Article 4. This Regulation shall be mandatory for all processing when:*
>
> *It is carried out in an establishment of the Data Controller in Mexican territory;*
>
> *It is carried out by a Data Processor, regardless of their location, on behalf of a Data Controller in Mexican territory;*
>
> *The Data Controller is not established in Mexican territory but the Mexican legislation is applicable to same derived from the execution of a contract or in terms of international law, and*
>
> *The Data Controller is not established in Mexican territory and uses means located in said territory, unless such means are used only for transit purposes that do not imply processing. For purposes of this subparagraph, the Data Controller shall provide the means necessary for the effective fulfillment of the obligations imposed by the Law, its Regulations and other applicable provisions, derived from the processing of personal data. For this purpose, it may designate a representative or implement the mechanism it deems pertinent, provided that it ensures that the Data Controller will be able to effectively comply, in Mexican territory, with the obligations that the applicable regulations impose to those entities that process personal data in Mexico.*
>
> *When the Data Controller is not located in Mexican territory, but the Data Processor is, the provisions related to the security measures contained in Chapter III of these Regulations will apply to the latter.*
>
> *In the case of individuals, the establishment will be understood as the place where the main seat of their business is located or the one they use for the performance of their activities or their home.*
>
> *In the case of companies, the establishment will be understood as the location where the main administration of the business is located; in the case of legal entities resident abroad, the location where the main administration of the business is located in Mexican territory, or in the absence thereof, the one they designate, or any stable installation that allows the effective or actual exercise of an activity."*

▪ *Consequently, provisions of the Mexican legal framework on data privacy can also be extraterritorial, as the GDPR. Furthermore, article 36 of the Law refers to transfers to third parties other than the Data Processors:*

> *"Article 36. Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating*

least the following information: I. The identity and domicile of the data controller collecting the data; II. The purposes of the data processing; III. The options and means offered by the data controller to the data owners to limit the use or disclosure of data; IV. The means for exercising rights of access, rectification, cancellation or objection, in accordance with the provisions of this Law; V. Where appropriate, the data transfers to be made, and VI. The procedure and means by which the data controller will notify the data owners of changes to the privacy notice, in accordance with the provisions of this Law. For sensitive personal data, the privacy notice must expressly state that it is dealing with this type of data."

(9) ARCO is an acronym used in Mexico and Spain for the rights of individuals to access, rectify, cancel and object to the use of their personal data in terms of the applicable law.

(10) Article 15 of the Law

(11) Article 3, subparagraph IX of the Law defines: "Data processor: The individual or legal entity that, alone or jointly with others, processes personal data on behalf of the data controller."

whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data."

▪ *Recently, Mexico was invited to enter into the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) of the European Council and its additional Protocol.*

Main issues in implementing GDPR in Mexico

▪ *GDPR requires the deploying of several actions worldwide to comply with its provisions when processing personal data of individuals covered by the EU GDPR.*

▪ *The main issues on the implementation of GDPR in Mexico for an entity are:*

- *To comply with technical and organizational measures, among others, regarding*
  - *the mapping of personal data,*
  - *eriod of storage of data,*
  - *pseudonymization and encryption of data,*
  - *data portability,*
  - *obligation to inform on a security breach and the plans, mechanisms to be put in place,*
  - *carry out DPIA when applicable to reduce violation of rights and freedoms of individuals,*
  - *analysis procedures to evidence consent and legitimate interest on data processing,*
  - *review and, if applicable, renegotiate with providers which have access to personal data,*
  - *assessment of domestic and international transfers, etc.;*
- *To update the obligations of the Chief Privacy Officer or Department of Personal Data to comply with GDPR provisions; and*
- *To update corporate governance in order to ensure the entity complies with GDPR and that employees are trained and updated.*

ENRIQUE OCHOA
DE GONZÄLEZ ARGÜELLES

mexico@
lexing.network

▪ Sur la définition de la donnée à caractère personnel donnée par le RGPD c'est la même que celle de la loi de 2008-12 sur les données à caractère personnel, sauf qu'il y a deux catégories de données prises en compte par le Règlement: la donnée de géolocalisation et l'identifiant en ligne.

▪ La course effrénée vers la conformité au 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 n'implique pas uniquement les entreprises de l'Union Européenne.

▪ En Afrique du nord et subsaharienne, beaucoup d'entreprises sont au même titre impactées par le RGPD, notamment celles qui sont dans le « Offshoring », les opérateurs de télécommunications, les banques et les prestataires de services informatiques.

▪ Les transferts de données à caractère personnel entre l'UE et des entreprises sénégalaises seront davantage encadrés à partir du 25 mai 2018. Actuellement les entreprises sénégalaises évoluant dans les domaines d'activités précitées sont non seulement régies par la loi sénégalaise n°2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel, mais elles sont dans l'obligation de se conformer au RGPD, au risque de disparaitre.

L'impact du RGPD

▪ La lecture combinée du considérant 23) et de l'article 3 du RGPD illustre son caractère extraterritorial. En vertu de l'article 3, le RGPD s'applique aux traitements de données à caractère personnel mis en œuvre par des sociétés sénégalaises, soit pour le compte de sociétés établies dans l'Union Européenne, soit que lesdits traitements concernent des personnes situées dans l'UE et sont relatifs à l'offre de biens ou de services, soumise à un paiement ou non.

▪ Au regard de ces dispositions, il y a deux catégories d'entreprises qui seront concernées :

- les entreprises sénégalaises, sous-traitants d'entreprises établies dans l'Union Européenne et ;
- les entreprises filiales de groupes d'entreprises établies dans l'UE.

▪ Pour les premières catégories d'entreprises, c'est-à-dire les sous-traitants, elles doivent présenter des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées, afin que le traitement soit conforme aux exigences du RGPD (respect des droits des personnes concernées, documentation de la conformité, etc.).

▪ Quant aux filiales sénégalaise de groupes, telles que les banques ou opérateurs de télécommunications, elles seront dans l'obligation d'appliquer les mesures de conformité au RGPD du groupe, notamment les BCR.

▪ Par ailleurs, en dehors de l'impact du RGPD sur les entreprises sénégalaises sous-traitants et filiales, les transferts de données à caractère personnel de l'UE vers des entreprises sénégalaises seront reconsidérées avec le RGPD.

▪ Ces transferts de données seront fondées soit sur une décision d'adéquation

du niveau de protection qu'offre le Sénégal, soit moyennant des garanties appropriées que présente le responsable de traitement établi dans l'UE. Ces garanties appropriées sont, entre autres, des règles contraignantes d'entreprises ou BCR, des clauses de types de protection, des codes de conduite et un mécanisme de certification.

Les enjeux de conformité

- Les entreprises sénégalaises impactées par le RGPD seront suivies de très près par leurs partenaires européens dans la mise en œuvre de la conformité. Ceci, notamment en raison des sanctions élevées que les entreprises non conformes peuvent subir, pouvant aller jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent.

- Aussi, pour ne pas perdre de partenaires européens au profit d'entreprises d'Afrique du nord, les entreprises sénégalaises doivent s'intéresser davantage à la conformité en matière de protection de données personnelles.

- Pour cela, elles peuvent désigner en interne ou en externe des délégués à la protection des données personnelles (DPO) qui seront, entre autres, chargés de mettre en place une documentation sur la conformité, de l'élaboration d'un registre des traitements, de l'analyse d'impact des traitements (DPIA).

- Par ailleurs, les entreprises concernées peuvent se rapprocher de la Commission de protection des Données personnelles du Sénégal (CDP) pour être accompagnées dans la conformité.

MAMADOU SEYE

senegal@
lexing.network

▪ *The definition of personal data given by the GDPR is virtually the same as the one contained in the Senegalese Personal Data Protection Act 2008-12, except that the GDPR contains two additional categories of personal data: location data and online identifier.*

▪ *The frantic race towards compliance with 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 does not only concern European companies.*

▪ *In North and Sub-Saharan Africa, many companies are equally impacted by the GDPR, particularly those engaged in offshoring activities, telecommunications operators, banks and IT service providers.*

▪ *Transfers of personal data between the EU and Senegalese companies will therefore be increasingly regulated from 25 May 2018. This means that Senegalese companies operating in the above lines of business will not only be required to comply with the Senegalese Personal Data Protection Act No. 2008-12 of 25 January 2008, but also with the GDPR, or else their business will disappear.*

Impact of the GDPR

▪ *The combined reading of recital (23) and Article 3 of the GDPR shows its extraterritorial nature. According to its Article 3, the GDPR applies to the processing of personal data by Senegalese companies either on behalf of companies established in the European Union, or to processing concerning individuals located in the EU in relation to the offering of goods or services, to such individuals, irrespective of whether a payment is required.*

▪ *In the light of these provisions, two categories of undertakings will be concerned:*

- *Senegalese companies that are the processors of companies established in the European Union and;*
- *subsidiaries of groups of companies established in the EU.*

▪ *For the first category, i.e. processors, they must provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR (respect the rights of data subjects, be able to demonstrate company, etc.).*

▪ *For the second category, i.e. Senegalese subsidiaries of EU groups, such as banks or telecommunications operators, will be required to apply the measures taken by the group to be GDPR compliant, such as in particular Binding Corporate Rules ("BCR").*

▪ *Furthermore, apart from the impact of the GDPR on Senegalese processors and subsidiaries, the transfers of personal data from the EU to Senegalese companies will also have to be reconsidered in the light of the provisions of the GDPR.*

▪ *Those data transfers will either be based on a decision on the adequacy of the level of protection offered by Senegal, or be subject to the provision of appropriates safeguards from the controller established in the EU, including BCR, standard data protection clauses, codes of conduct and a certification mechanism.*

Compliance issues

- *The European partners of Senegalese companies impacted by the GDPR will closely monitor how implement their compliance. This is due in particular to the high penalties that non-compliant companies can face, which can reach up to 4% of the total worldwide annual turnover of the preceding financial year.*
- *As a result to avoid losing European partners to North African companies, Senegalese companies must pay more attention to compliance in terms of personal data protection.*
- *To this end, they may appoint internal or external data protection officers (DPOs) who will notably be responsible for setting up compliance documentation, maintain a record of processing activities and carry out a data protection impact assessment (DPIA).*
- *In addition, the companies concerned may approach the Senegalese data protection commission (Commission de protection des Données personnelles du Sénégal, or CDP) for guidance for GDPR compliance.*

MAMADOU SEYE

senegal@
lexing.network

▪ Le RGPD suscite un vif intérêt en Russie. Certes, la Russie est en dehors de l'Union européenne et l'autorité russe de protection des données ne reconnaît pas l'applicabilité du RGPD sur le territoire russe, mais ce règlement européen n'en reste pas moins un sujet d'une brûlante actualité tant pour les entreprises russes ayant des activités commerciales sur le territoire de l'UE que pour les filiales d'entreprises européennes ayant des activités commerciales sur le territoire de la Russie.

▪ Les entreprises russes doivent par conséquent veiller à harmoniser la conformité de leurs activités de traitement de données à la fois avec les exigences de la législation européenne et les exigences de la législation russe.

Double charge imposée aux responsables du traitement russes

▪ Les responsables du traitement russes qui sont soumis au RGPD se voient ainsi confrontés au doublement de leurs obligations, car ils doivent assurer la conformité de leurs systèmes avec les obligations légales russes ainsi qu'avec les nouvelles exigences européennes en matière de protection des données.

▪ Par certains côtés, les législations de l'UE et de la Russie se rejoignent. Par exemple, la loi russe sur la protection des données et le RGPD exigent tous deux de procéder à un inventaire exhaustif des activités de traitement des données opérées, même si l'étendue des informations à analyser et la méthode d'analyse préconisées par chaque texte divergent. En outre, en Europe et en Russie, le responsable du traitement des données est tenu d'élaborer diverses politiques et procédures, et de réaliser certaines formalités d'obtention de consentement des personnes concernées afin de justifier ses activités de traitement et démontrer le respect de ses obligations légales.

▪ De manière générale, les dispositions du RGPD et de la loi russe sur la protection des données ne se contredisent pas. De cette manière, les responsables du traitement russes peuvent utiliser les mêmes procédures de traitement, les mêmes politiques de protection des données, les mêmes formulaires de consentement au traitement des données... pour la Russie et l'UE.

▪ Toutefois, les deux textes présentent également leurs différences. Par exemple, en Russie, les responsables du traitement sont tenus de transmettre les informations concernant leurs activités de traitement à l'autorité de protection des données, qui publie ensuite ces informations dans un registre public. En revanche, dans le cadre du RGPD, c'est le responsable du traitement qui est en charge de tenir un registre de ses activités de traitement. Par ailleurs, s'agissant du transfert de données de salariés au sein d'un groupe d'entreprises, le RGPD met en place un mécanisme des règles d'entreprise contraignantes, tandis que la législation russe conditionne la légitimité de ces transferts intra-entreprise à la signature d'accords entre responsables du traitement et sous-traitants et à l'obtention du consentement écrit des salariés.

▪ Enfin, le RGPD prévoit certaines procédures qui n'ont pas d'équivalent dans la loi russe. Parmi celles-ci figure l'obligation de signaler les violations de données à l'autorité compétente dans les 72 heures.

▪ Dans ces conditions, les responsables du traitement russes se retrouvent pris entre deux feux et devront réaliser un gros travail de mise en balance en vue de trouver un équilibre leur permettant de rester dans les clous et satisfaire à la fois les exigences opérationnelles tenant au fonctionnement des entreprises russes et européennes et les exigences réglementaires édictées par les autorités de contrôle.

Les lacunes de la législation russe

▪ Même si les principales obligations qu'elles renferment sont très similaires à celles contenues dans le RGPD, la loi russe sur la protection des données apparaît quelque peu désuète au regard de la réalité numérique. En particulier, le législateur russe ne traite pas suffisamment en profondeur de questions telles que le profilage, le droit à la portabilité et le droit à l'oubli, ni de tous les aspects des flux transfrontières de données. Ne sont également pas abordées les relations entre responsables du traitement, la qualification de responsables conjoints du traitement, ou encore les données génétiques, les données anonymes et les données pseudonymisées.

▪ Lorsque les responsables du traitement russes relevant du RGPD se retrouvent confrontés à ces thématiques pour lesquelles les lois russes ne prévoient qu'une réglementation très limitée, voire inexistante, ils sont tenus d'appliquer les instruments prescrits par le RGPD, tout en ne perdant pas de vue que l'autorité russe de protection des données ne reconnaît pas l'application du RGPD sur le territoire russe. Les responsables du traitement russes se trouvent dès lors dans une position floue et délicate pour faire valoir la conformité à la loi russe de leurs instruments conformes au RGPD.

La conception imprécise d'« intérêt légitime » en Russie

▪ Pour le RGPD, un « intérêt commercial légitime » peut constituer une base juridique pour le traitement de données à caractère personnel. Pour la loi russe, le traitement de données personnelles est possible lorsqu'il est nécessaire à la réalisation des « droits et intérêts légaux » du responsable du traitement ou de tiers, et notamment lorsque cela est prévu par la loi fédérale sur la protection des droits et intérêts légitimes des personnes physiques dans le cadre du recouvrement de créances ou lorsque cela est nécessaire afin d'atteindre des objectifs d'importance publique, à moins qu'il ne soit porté atteinte aux droits et libertés de la personne concernée.

▪ Or, la question de savoir quels droits et intérêts légaux peuvent constituer un motif de traitement des données n'est clarifiée ni par les régulateurs ni par les tribunaux russes. En outre, il n'existe pas non plus de test de mise en balance entre les droits et libertés de la personne concernée et les droits et intérêts légitimes du responsable du traitement ou de tiers, qui permettrait de trancher en cas de conflit. Dans ces conditions, il n'est pas clair dans quels cas « l'intérêt commercial légitime » posé par le RGPD pourrait être transposé dans le cadre juridique russe, hormis en cas d'exercice des activités liées au remboursement de dettes en souffrance.

▪ En raison de cette incertitude, les responsables du traitement russes se voient souvent contraint d'obtenir le consentement des personnes concernées afin de justifier leur traitement, alors que dans le cadre du RGPD ce même traitement peut être effectué sur la base de l'intérêt commercial légitime du responsable du traitement.

MARIA OSTASHENKO
&
ANASTASIA PETROVA

russia@
lexing.network

▪ *Although Russia is outside the EU and Russian Data protection authority does not recognize the GDPR applicability in Russia, GDPR is a very hot topic for Russian companies conducting business in the EU and subsidiaries of the EU companies conducting business in Russia.*

▪ *Russian companies have to bring their data processing activities in harmonized compliance with both GDPR and Russian legal requirements.*

Double Burden for Russian controllers

▪ *Russian data controllers falling under the GDPR will face double burden in terms of bringing their processes in compliance with both Russian and new European data protection requirements.*

▪ *Both Russian data protection law and GDPR require extensive inventory of data processing activities as a primary step for achievement of compliance. However, the scope of information to be analyzed under Russian law and the GDPR, as well as approach to the analysis, differs. Further, data controller shall elaborate and implement policies, procedures, notices, consents and agreements, which justify its data processing activities and demonstrate compliance with legal obligations under both GDPR and Russian data protection laws.*

▪ *Generally GDPR and Russian data privacy regulations do not contradict each other. Thus, Russian controllers may have single data processing policies, privacy notices, data processing consent forms.*

▪ *However a number of procedures differs under the GDPR and Russian data protection law. Russian data controllers are obliged to file the information about data processing activities to the Data protection authority, which publish this information in public registry. Under the GDPR data controller shall maintain records of processing activities itself. GDPR provides for Binding Corporate Rules as a mechanism of employee data transfer inside the group of companies. Russian law requires signing of controller-to-processor agreements and obtaining employee written consents in order to ensure legitimate ground for intra-group data transfers.*

▪ *GDPR provides for certain procedures, which are not addressed in Russian privacy laws. Among them the notifications on data breaches, which have to be provided to the relevant regulator within 72 hours.*

▪ *Considering the above Russian controllers will have to make a big job in order to find a balance, where both Russian and European businesses and data protection regulators feel equally satisfied.*

Russian law does not provide sufficient regulations

▪ *Although basic requirements of the GDPR are very similar to requirements of Russian data protection law, Russian data protection law is outdated for our digital reality. In particular, Russian law does not address sufficiently such matters as profiling, right of portability and right to be forgotten, comprehensive regulations on cross-border transfer of personal data, controller*

to controller relations and co-controllers, genetic data, regulation of anonymized and pseudonymized data.

- *When Russian controllers falling under the GDPR face with the above issues in course of their business activities they do need to apply GDPR instruments to regulate such processing. Russian laws provide for very limited or lack of regulation on such processing. With that Russian Data protection authority does not recognize GDPR effective in Russia. In such circumstances Russian data controllers are in very unclear and challengeable position regarding recognition of their GDPR instruments complied with Russian laws.*

Unclear conception of "legitimate business interest" in Russia

- *GDPR recognizes "legitimate business interest" as a legitimate ground for significant scope of data processing activities of controllers. Russian Data Protection Act permits processing of personal data for the purpose of exercising the rights and lawful interests of the data controller or third persons, including where it is provided for by the Federal Law on the Protection of Natural Persons' Rights and Legitimate Interests When Exercising the Activities Involved in Return of Overdue Debts, or for the purpose of attaining goals of public importance, unless in this case the rights and freedoms of the personal data subject are infringed upon.*

- *The question what rights and lawful interests can be a ground for data processing is not clarified by Russian regulators of courts. Also there is no balancing test between the rights and freedoms of the personal data subject and rights and lawful interests of the data controller or third persons. Thus, it is not clear in which cases "legitimate business interest" can apply, except for the cases of exercising the activities involved in return of overdue debts.*

- *Due to the above uncertainty Russian data controllers often have to rely on consent of a data subject when under the GDPR the processing can be conducted based on the legitimate business interest of the data controller.*

MARIA OSTASHENKO
&
ANASTASIA PETROVA

russia@
lexing.network

LEXING NETWORK

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne *Germany*	Beiten Burkhardt	Andreas Lober	+49 69 756095-0	germany@lexing.network
Australie *Australia*	Madgwicks Lawyers	Dudley Kneller	+61 3 9242 4744	australia@lexing.network
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Jean-François De Rico	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Costa Rica *Costa Rica*	Lexing Costa Rica	Gabriel Lizama	+506 2253-1726	costa-rica@lexing.network
Côte d'Ivoire *Ivory Coast*	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
États-Unis *USA*	Greenberg Traurig	Françoise Gilbert	+1 650-804 1235	usa@lexing.network
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Inde *India*	Poovayya and Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Israël *Israel*	Appelfeld & Co	Ilanit Appelfeld	+ 972 3 60 98 099	israel@lexing.network
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Maroc *Morocco*	Fayçal Elkhatib et Associés S.C.P.A	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Arve Føyen	+47 21 93 10 00	norway@lexing.network
Nouvelle-Calédonie *New Caledonia*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	nc@lexing.network
Pologne *Poland*	Traple Konarski Podrecki i Wspòlnicy	Xawery Konarski	(+48) 12 426 05 30	poland@lexing.network
Portugal *Portugal*	Alves Pereira & Teixeira de Sousa	João P. Alves Pereira	+ 351 21 370 01 90	portugal@lexing.network
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Russie *Russia*	ALRUD	Maria Ostashenko	+ +7 495 234 96 92	russia@lexing.network
Sénégal *Senegal*	SCP Faye & Diallo	Mamadou Seye	:(+221) 33 823 60 60	senegal@lexing.network
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network
Tunisie *Tunisia*	Younsi & Younsi International Law Firm	Yassine Younsi	+216 98 37 37 28	tunisia@lexing.network

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan
Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier
Diffusée uniquement par voie électronique – gratuit –
ISSN 1634-0701
Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/

Crédit photo / Photo credit : Privacy concept- Data Protection on digital background@Maksim Kabakou – Fotolia