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°16 – octobre 2017
JTIT Special international issue #16 – October 2017

CONFERENCE LEXING SUR LE RGPD

LEXING CONFERENCE ON GDPR

RGDP : LE COMPTE A REBOURS EST LANCE, J-230 !

- Dans le cadre de leur 6e conférence annuelle, les membres du réseau Lexing® ont organisé le 15 juin 2017 à Milan, en Italie, une conférence-débat consacrée au Règlement général sur la protection des données (RGPD).
- L'occasion, à moins d'un an de l'entrée en application de ce texte qui va modifier en profondeur les règles applicables à l'environnement digital des entreprises privées et organismes publics, d'aborder les enjeux pour les entités européennes mais aussi celles hors de la zone Europe. Les membres du réseau ont utilisé la tribune qui leur était ainsi offerte pour exposer leur vision des enjeux du règlement européen à l'aune de leurs pays respectifs. Ils ont eu l'honneur de confronter leurs points de vue avec celui des autorités et des professionnels invités pour l'occasion (avocats, membres des autorités de protection des données, magistrats, juristes de grandes entreprises multinationales).
- Le texte entrera en application le 25 mai 2018. Le compte à rebours a donc commencé !
- Tous les membres du réseau vous donnent d'ores et déjà rendez-vous à Paris (France), pour une nouvelle conférence, en juin 2018.

Ce numéro vous propose, de manière synthétique, une sélection des interventions qui ont eu lieu à l'occasion de cette conférence.

GDPR: THE COUNTDOWN IS ON, D-230!

- *On 15 June 2017, the Lexing® network members held their 6th annual conference in Milan (Italy) dedicated to the General Data Protection Regulation (GDPR).*
- *This was the opportunity to review the stakes of the GDPR, less than a year from its entering into application, as it will drastically change the whole digital world and impact directly on any public or private organisation, independently from it being EU-based or not. The network members used that forum to each give a unique insight into the challenges and opportunities raised by the GDPR based on the specificities of their respective country. They had the honour to share their views with special guests and speakers invited to attend the conference (members of the data protection authorities, judges, in-house counsels of large multinational corporations).*
- *The GDPR will come into force on 25 May 2018. The countdown is on!*
- *Come and join us at our next Lexing conference, which will take place in Paris (France) in June 2018. Save the date!*

This issue brings together a selection of brief articles summarizing some of the presentations given at the conference.

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

FREDERIC FORSTER
Vice-président du réseau Lexing® et Directeur du pôle Constructeurs Informatique, Télécoms et Electronique du cabinet Lexing Alain Bensoussan-Avocats

VP of Lexing® network
Head of the IT and Telco division
of Lexing Alain Bensoussan-Avocats

Introduction

▪ Le règlement général sur la protection des données 2016/679 du 27 avril 2016, dit « RGPD », va bientôt profondément modifier les règles applicables au traitement et à la protection des données à caractère personnel, bien au-delà des frontières de l'Union européenne.

▪ Véritable bouleversement dans le monde du numérique, ce règlement va obliger tous les organismes qui opèrent dans un contexte mondial à adopter une approche complètement nouvelle des données à caractère personnel. En effet, le RGPD ne concerne pas que les entreprises européennes, puisqu'il vise également tout organisme exerçant des activités ou offrant des services sur le territoire européen, et ce qu'il soit ou non établi dans un pays membre de l'UE.

▪ Depuis la directive communautaire du 24 octobre 1995, les technologies ont évolué conduisant à une augmentation exponentielle du partage des données à caractère personnel. Le RGPD a vocation à moderniser le cadre européen de la protection des données à caractère personnel afin de prendre en compte les avancées technologiques notamment numériques et génétiques et de réduire les écarts juridiques entre les différentes législations des Etats membres de l'Union européenne.

▪ La place grandissante d'internet dans les foyers européens et l'émergence de l'utilisation des réseaux sociaux et des objets connectés requièrent de réviser le cadre légal de la protection des données à caractère personnel, afin de l'adapter à ces nouveaux modes d'utilisation des données. De plus, les données sont au centre de l'activité de nombreuses entreprises. Le RGPD poursuit un double objectif : créer la confiance des personnes concernées sans pour autant mettre de freins à l'activité économique et au développement des entreprises européennes.

▪ De nombreux acteurs vont ainsi être amenés à repenser leurs politiques en matière de protection des données afin de prendre en compte ce texte qui renforce considérablement les obligations des entreprises, tout en améliorant la protection accordée aux individus. Si les formalités déclaratives sont simplifiées, les obligations des responsables de traitement sont en revanche renforcées pour assurer une meilleure protection des données à caractère personnel.

▪ Les dispositions du RGPD seront directement applicables dans les Etats membres de l'Union européenne à compter du 25 mai 2018. A moins d'un an de l'entrée en application de ce texte, Lexing®, premier réseau international d'avocats en droit du numérique et des technologies, a organisé, le 15 juin 2017, à Milan (Italie), une Conférence-débat ouverte à tous afin de décrypter les nouvelles règles, et permettre d'anticiper et d'organiser les actions de mise en conformité, ainsi que de dialoguer avec d'autres acteurs confrontés aux mêmes problématiques.

▪ Venus du monde entier, les membres du réseau ont eu l'honneur de confronter leurs points de vue avec celui des autorités et des professionnels invités pour l'occasion :

- Giovanni Buttarelli, contrôleur européen de la protection des données,
- Francesco Cajani, procureur de la République de Milan,
- Fabio Rastrelli, directeur de la Conformité à la Banca Intesa,
- Alberto Caselli, membre de l'Autorité italienne de la protection des données,
- Roberto De Simone, conseiller juridique chez SKY Italie, et
- Marc Mossé, Directeur Affaires Juridiques et Affaires Publiques chez Microsoft.

▪ Les débats ont principalement porté sur les thèmes suivants, objets d'autant de tables rondes : les nouvelles exigences de la protection des données dès la conception, le principe d'accountability et les sanctions renforcées encourues, les questions relatives aux transferts de données dans un monde sans frontières ainsi que le rôle spécifique du délégué à la protection des données ou DPO, nouveau personnage clé de l'environnement digital des entreprises.

Après le succès de cet évènement, nous vous donnons rendez-vous à Paris, en France, en juin 2018, pour notre prochaine conférence Lexing.

ORATEURS

Alain Bensoussan
Lexing France
france@lexing.network
Fondateur et président du réseau Lexing®

Raffaele Zallone
Lexing Italie
italy@lexing.network
Pays organisateur de la conférence de Milan

Discours prononcé par Giovanni Buttarelli, contrôleur européen de la protection des données (CEPD)

Introduction

▪ *The General Data Protection Regulation 2016/679 of 27 April 2016, known as "GDPR", will drastically change the ways you may process and must protect personal data in Europe and beyond.*

▪ *The GDPR will impact the whole digital world and will require a completely new approach to data privacy in day-to-day operations, on the workplace and on the web, for anyone who operates in a global context. When in force, the GDPR will uniformly apply all over Europe but will impact directly on any organization doing business in Europe, independently from its being EU-based or not.*

▪ *Since the Directive of 24 October 1995, technologies have changed dramatically and led to exponential growth in the sharing of personal data. The GDPR is intended to modernise existing EU data protection framework to bring it in line with new technological developments, including in the digital and genetic fields, and reduce legal differences between the various laws of the EU Member States.*

▪ *The growing role of the internet in European households and the emergence of social networks and connected devices required revising the legal framework for data protection in order to adapt to these new ways of using data and make Europe fit for the digital age. Data are at the core of many companies' business. The GDPR pursues a twofold objective: create trust among stakeholders without hampering the economic activity and development of European enterprises.*

▪ *In addition, the GDPR significantly modifies several obligations for organisations while strengthening the protection for individuals, with obvious impact on the way organisations have coped with privacy up to now. While it cuts through red tape, some obligations are also strengthened with the aim of ensuring better data protection safeguards.*

▪ *The provisions of the GDPR will be directly applicable in all Member States of the European Union starting 25 May 2018. Less than a year from its application, Lexing®, the first international lawyer's network specialized in emerging and technology law, organized a public conference on 15 June 2017 to allow you to obtain an overview of the new rules, plan what action you need to take to comply, and network with others facing the same challenges as you.*

▪ *Coming from all over the world, Lexing's lawyers had the honour to share their views with the special guests and speakers invited to attend the Lexing 2017 GDPR Conference:*

- *Giovanni Buttarelli, European Data Protection Supervisor,*
- *Francesco Cajani, Procuratore della Repubblica (Milan),*
- *Fabio Rastrelli,, Chief Compliance Officer, Banca Intesa (Milan),*
- *Alberto Caselli, Garante Privacy (Rome),*
- *Roberto De Simone, Legal Adviser at SKY Italy, and*
- *Marc Mossé, Director of Legal and Public Affairs at Microsoft at Microsoft.*

▪ *Discussions were mainly focused on the following topics: the new "privacy by design" requirements, the principle of "accountability" and the sanctions incurred for non-compliance, data transfers issues in an open world, and the new key role of the DPO (data protection officer).*

After the success of this event, we have the pleasure invite you to join us for the next Lexing annual conference, which will take place in Paris (France) in June 2018.

SPEAKERS

Alain Bensoussan
Lexing France
france@lexing.network
Founder and president of the Lexing® Network

Raffaele Zallone
Lexing Italy
italy@lexing.network
Organising country of the Milan conference

Keynote Speech by Giovanni Buttarelli, European Data Protection Supervisor (EDPS)

Protection des données dès la conception

INTERVENANTS

▪ L'article 25 du règlement général sur la protection des données (RGPD) impose aux responsables du traitement de mettre en œuvre des mesures techniques et organisationnelles propres à assurer la protection des données et des droits des personnes concernées dès la conception d'un produit ou d'un service (principe dit de « protection des données dès la conception » ou de « privacy by design »). Autrement dit, une entreprise doit respecter les principes posés par le RGPD à l'égard de toutes les données à caractère personnel qu'elle collecte, utilise, stocke, transmet ou supprime tout au long du cycle de vie de son produit, depuis sa conception jusqu'à son exploitation. A cette fin, les mesures auxquelles elle peut recourir incluent, par exemple, la minimisation des données, la limitation des durées de conservation des données ou encore la mise en place d'une politique de sécurité des données. L'article 25 exige également des responsables du traitement qu'ils ne traitent les données à caractère personnel que dans un but précis (principe de « protection des données par défaut »). Protection des données dès la conception et protection par défaut, tels sont les deux principes clés de la conformité d'un produit ou d'un service au RGPD.

Protection des données dès la conception

▪ La première étape de la protection des données dès la conception consiste à évaluer les finalités et les fonctionnalités du produit envisagé, les catégories de données pouvant être collectées ainsi que les modalités prévues pour le partage, la conservation ou la suppression de ces données. Seul l'établissement d'une cartographie claire et détaillée, recensant et identifiant les catégories de données collectées, les catégories de destinataires des données et l'utilisation prévue des données permettra d'appréhender l'effet potentiel du produit sur les droits à la vie privée des utilisateurs finaux et des autres acteurs concernés.

▪ Une fois établie, cette cartographie fera, dans une seconde étape, l'objet d'une analyse qui permettra de déterminer si, et dans quelle mesure, les activités envisagées respectent les principes en matière de protection des données énoncés par le RGPD. C'est à cette occasion que seront soulevées des questions essentielles, telles que : les données dont la collecte est envisagée sont-elles acquises « de manière loyale et licite » ? Existe-t-il une base légale justifiant la collecte des données, ou doit-on mettre en place un processus technique permettant de recueillir le consentement de l'utilisateur final à l'utilisation de ses données ? De quelle manière obtenir ce consentement tout en offrant une bonne expérience utilisateur ? Le volume de données recueillies est-il proportionné au regard du bon fonctionnement du produit, ou est-il possible de réduire ou modifier la quantité ou la nature des données collectées afin de s'assurer que la collecte se limite aux seules informations strictement nécessaires ?

▪ D'emblée, il conviendra de définir des mesures de sécurité efficaces et les intégrer au logiciel ou à toute autre technologie utilisée dans le produit ou la prestation de service. Il est essentiel de maintenir un niveau de sécurité adéquat tout au long du cycle de vie du produit. Concrètement, cela peut se traduire par des mesures d'authentification pour limiter l'accès et la modification des données aux seules personnes habilitées. Il faudra, en outre, ne pas oublier de prévoir les modalités de suppression des données lorsque la fabrication du produit sera abandonnée ou le service résilié, et intégrer ces modalités au codage informatique, pour s'assurer que toutes les informations stockées dans les bases de données associées, la mémoire ou tout autre périphérique de stockage soient supprimées de manière appropriée et sécurisée.

Marc Mossé
Directeur Affaires Juridiques
et Affaires Publiques
Microsoft Corporation

Francoise Gilbert
Lexing USA
usa@lexing.network

Sébastien Fanti,
Lexing Suisse
switzerland@lexing.network

Modérateur :

Daniel Preiskel
Lexing UK
uk@lexing.network

▪ Enfin, la durée de conservation des données devrait être limitée tant au moment de la phase de conception initiale qu'ultérieurement lors de ses mises à jour, afin de s'assurer que les données soient conservées uniquement pendant la durée minimum nécessaire, non seulement afin d'éviter de conserver des données inutiles, mais également en vue de réduire les risques de vol ou de perte. Le risque important de violation de sécurité justifie de porter une attention particulière aux mesures de sécurité (caractéristiques détaillées, variété et flexibilité), dès les premiers stades de développement du produit.

Protection des données par défaut

▪ La conception du produit doit également se faire dans le respect du principe de « protection des données par défaut » (« privacy by default) fixé au paragraphe 2 de l'article 25 du RGPD. Ce principe impose de configurer les paramètres initiaux du produit de sorte que, par défaut, les niveaux les plus élevés de confidentialité, de sécurité et de protection des données soient offerts à l'utilisateur final. Concrètement, cette démarche suppose, par exemple, de limiter la quantité des données collectées automatiquement. Le produit doit donc être conçu de telle manière à ce que, par défaut, les données à caractère personnel ne soient pas rendues accessibles, par inadvertance, à un nombre indéterminé de personnes. En particulier, les paramètres initiaux du produit doivent interdire la divulgation, le partage ou l'accès des données à des tiers sans l'intervention préalable de la personne concernée.

Intégration en harmonie avec les structures existantes

▪ L'élaboration et l'analyse de la cartographie des données doivent se faire au regard des politiques déjà applicables au sein l'entreprise en matière de protection des données et de la vie privée afin de s'assurer que la collecte, le stockage, le traitement ou le partage envisagés s'inscrivent bien dans les valeurs et principes de l'entreprise. En cas d'écarts constatés, un ajustement du produit envisagé ou des documents et politiques existants sera nécessaire.

Méthodologie

▪ Pour s'assurer d'appliquer de manière exhaustive les principes de protection dès la conception et par défaut, il est possible de s'inspirer de la méthodologie utilisée dans le cadre de l'analyse d'impact relative à la protection des données. Ces éléments contribuent à déterminer dans quelle mesure le traitement envisagé est susceptible de poser des risques pour la vie privée des individus ou la sécurité de leurs données. A l'issue de cette démarche, l'entreprise sera ainsi en position de dresser une liste de critères, de restrictions ou de conditions à respecter lors de conception et le développement du produit, ainsi que tout au long de son cycle de vie dans le respect du RGPD.

Conclusion

▪ Les principes de protection des données dès la conception et par défaut encadrent de manière substantielle le développement et l'exploitation d'un produit ou d'un service. Ils sont la traduction concrète des principes généraux de protection d'ores et déjà consacrés par la plupart des lois sur la protection des données en Europe, ainsi que dans les « fair information practices principles » aux Etats-Unis. Ils participent à la création d'une base solide sur laquelle mettre en balance l'intérêt ou le droit légitime des personnes physiques à protéger leurs données à caractère personnel, avec les objectifs, commerciaux ou non, des entreprises qui collectent et traitent ces données.

Synthèse préparée par :
Françoise Gilbert

Privacy by design

PANELISTS

▪ *Article 25 of the EU General Data Protection Regulation (GDPR) imposes on controllers an obligation to use appropriate technical and organizational measures that are designed to implement the data protection principles and protect the rights of the data subjects. This process, known as "data protection by design" requires that at all stages of the development, implementation, and operation of a product, the responsible entity ensures that the collection, use, storage, transmittal, or deletion of personal data is conducted in accordance with the GDPR, including, for example, data minimization, limited retention or appropriate data security. Article 25 also requires that controllers ensure that, by default, only the personal data that is necessary for a specific purpose are processed. These two elements are the foundation of the design of a GDPR compliant product.*

Data Protection by Design

▪ *Data Protection by Design starts with evaluating the purposes and functionality of the proposed product, the categories of data that might be collected, and the intended uses, sharing, retention, or disposal of the data. Only a clear and detailed flowchart identifying the different components of the design, the categories of data collected, the categories of recipient of the data, and the intended use of the data, will allow understanding the potential effect of that design on the privacy rights of the end-users and other affected parties.*

▪ *The flowchart should be analyzed to determine whether, and the extent to which, the proposed activities meet the GDPR data protection principles. For example, is all data that is proposed to be collected acquired "fairly and legally"? Are there any legal justifications that allow the collection of the data? Or should there be a technical process in place to allow the end-user to consent to the use of the data? How should that consent be obtained to ensure adequate user experience? Is the amount of data collected appropriate for the proper operation of the product? Or should the amount or nature of the data collected be reduced or modified to ensure that only the information that is strictly necessary is collected?*

▪ *From the earliest stage of conception and development, sound security measures should be identified and encoded in the software or other technology used in the product or as part of the service. Adequate security must be present in the entire life cycle. For example, access to data should be guarded with appropriate authentication measures, and modification of existing data should be allowed only to specified individuals. Disposal of data, when the product or service is dismissed or terminated, should be planned and programmed accordingly, and incorporated within the coding, so that all data stored in the associated databases, memory, or other storage devices is properly and securely deleted.*

▪ *The duration of data retention should be limited both as part of the original design and subsequent updates to that design, to ensure that data is kept for the minimum amount of time necessary, thereby avoiding the retention of unnecessary data and reducing the risk of theft or loss. Attention to the detail, variety, and flexibility of security measures from the early stages of development is especially important in view of the substantial risk of a breach of security.*

Marc Mossé
Directeur Affaires Juridiques
et Affaires Publiques
Microsoft Corporation

Francoise Gilbert
Lexing USA
usa@lexing.network

Sébastien Fanti
Lexing Switzerland
switzerland@lexing.network

Moderator:

Daniel Preiskel
Lexing UK
uk@lexing.network

Data Protection by Default

▪ *The design should also incorporate the proper analysis and processes for ensuring "data protection by default," as required by GDPR Article 25(2). "Data protection by default" requires that the initial settings be set, so that, by default, the highest levels of privacy, security, and data protection are provided to the end user. This would include, for example, limiting the amount of information that is automatically collected. The design should ensure that personal data is not inadvertently made accessible to an unlimited number of persons by default. Instead, the initial product settings should prohibit disclosure, sharing or access and should require the prior intervention of the concerned individual before the data can be disseminated or disclosed to others.*

Integration with Existing Structures

▪ *The review of the different aspects of the flowchart should take into account the existing privacy policy of the company to ensure that the proposed collection, storage, processing or sharing is in line with the company's existing privacy and data protection values. If there are discrepancies, the product or these documents and policies would have to be updated accordingly.*

Methodology

▪ *To ensure that all important aspects are covered, the review could be organized using the same methodology as that which is used to conduct data protection impact assessments. This will help determine the extent to which the proposed processing is likely to pose risks to the privacy of individuals or the security of their personal information. In the end, the analysis described above should result in the creation of a list of requirements, restrictions or conditions to be followed in the design and development of the product and throughout the entire period during which the product is put in use.*

Conclusion

▪ *Data protection by design and by default principles provide important guidance for the development and operation of a product or service. They translate into practical application the general principles that are found in most data protection laws, and in the fair information practices principles, as well. They help guide the creation of a solid base that helps balance the legitimate interest or right of individuals in protecting the privacy and security of their personal information and the business and other objectives of companies collecting and processing the data.*

Summary prepared by:
Françoise Gilbert

Le délégué à la protection des données (DPO)

INTERVENANTS

▪ Une des principales innovations du RGPD est la création de la fonction de délégué à la protection des données, souvent désigné par l'acronyme DPO, « data protection officer » en anglais. Le DPO soulève de nombreuses questions au sein des entreprises ou organismes qui doivent assurer la mise en conformité de leur organisation avec les règles du texte européen : qui désigner pour occuper ce poste ? Sous quel délai ? Quelles seront exactement ses missions et ses responsabilités ?

▪ Le principe de responsabilité, ou d'« accountability », est au cœur du RGPD. Ce principe, qui impose aux responsables du traitement et aux sous-traitants d'adopter des mesures concrètes en matière de vie privée, va forcer les entreprises à mettre l'accent sur le fond plutôt que sur la forme. Ils sont en effet dans l'obligation non seulement de mettre en œuvre des mesures appropriées et effectives, mais également d'être à même de démontrer la conformité de leurs activités de traitement avec le RGPD, en tenant compte de tous les spécificités de leur structure et des traitements. Or, chaque traitement est unique et peut impliquer des risques différents pour les personnes concernées, qu'il convient d'analyser et d'évaluer pour prendre des mesures appropriées.

▪ Dans ce contexte, le DPO apparaît comme un moyen d'accompagner les entreprises dans leur démarche pour maîtriser ces risques. De toute évidence, au vu de son rôle particulier, le DPO devra nécessairement jouir d'une certaine indépendance, et posséder une connaissance technique approfondie du RGPD ainsi que de la structure interne et des activités de traitement de l'entreprise, afin de mieux appréhender les risques spécifiques en jeu.

▪ Grâce aux brillantes observations de ses intervenants, le panel de discussion consacré à la thématique du DPO a analysé le sujet sous deux angles principaux : un angle pratique, présenté par M. Rastrelli, chef du département de la sécurité et de la protection de la banque Intesa Sanpaolo, et un angle plus technique, développé par Me. Konstantakopoulos et Me. Henrotte, tous deux avocats membres du Réseau Lexing®, respectivement en Grèce et en Belgique.

▪ Dans un premier temps, l'approche pratique de M. Rastrelli a mis en lumière les différentes étapes à suivre afin d'organiser le suivi de toutes les activités de traitement au sein d'un groupe d'entreprises, étant rappelé que les responsables du traitement et sous-traitants sont tenus analyser le risque de chaque activité de traitement. Prenant l'exemple d'un groupe bancaire international, M. Rastrelli a expliqué qu'il était possible de nommer un DPO par entité juridique, dans chaque pays où la banque est implantée, ce réseau de DPO étant alors coordonné par un DPO groupe en charge de superviser les principaux aspects de mise en œuvre du RGPD.

▪ Dans un deuxième temps, Me. Konstantakopoulos a analysé les problématiques techniques concrètes soulevées par la fonction de DPO, notamment en termes d'implication, de ressources, d'indépendance et de conflits d'intérêts. Les entreprises ont encore du mal à comprendre le fonctionnement du DPO et la manière dont l'exigence d'indépendance peut être satisfaite dans la pratique. Le RGPD énonce clairement que le DPO ne reçoit aucune instruction en ce qui concerne l'exercice de ses missions, qu'il fait directement rapport au niveau le

Fabio Rastrelli
Chief Compliance Officer
Banca Intesa (Milan, Italie)

Jean-François Henrotte
Lexing Belgique
belgium@lexing.network

Theodore Konstantakopoulos
Lexing Grèce
greece@lexing.network

Modérateur :

Alfredo Zallone
Lexing Italie
italy@lexing.network

plus élevé de la direction, qu'il ne peut être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions. En outre, le DPO doit bénéficier des ressources nécessaires à l'exercice de l'ensemble de ses missions. Cela étant, dans les faits, l'indépendance du DPO pourrait être difficile à garantir : un marché du DPO va se nécessairement se développer et, par conséquent, il sera possible pour les organismes de trouver un DPO plus ou moins accommodant.

▪ Me. Henrotte, au regard de ces considérations, a ensuite relayé certaines interrogations de ses clients, notamment, en ce qui concerne la personne devant endosser la responsabilité des conseils dispensés et des actions menées par le DPO. D'après ce que nous savons, cette responsabilité revient aux responsables du traitement et aux sous-traitants. Ces derniers ne peuvent donc se défausser sur le DPO, ce qui les incitera d'ailleurs à être davantage à l'écoute des recommandations formulées par le DPO. Abordant un autre aspect important, Jean-François Henrotte a également expliqué comment le DPO devra gérer la confidentialité des informations qui lui sont transmises, et quel type de garanties contractuelles seront nécessaires afin de protéger son indépendance et prévenir tout licenciement abusif. A notre connaissance, les responsables du traitement et les sous-traitants qui relèveraient de ses fonctions un DPO n'encourraient aucune sanction civile, et pour éviter le risque de sujétion du DPO à l'égard de la direction de l'entreprise par peur de représailles, l'insertion d'une clause pénale au profit du DPO dans son contrat de travail pourrai être envisagée.

▪ Comme l'ont souligné les membres du panel à plusieurs reprises, le texte du RGPD est loin d'être parfait et laisse une large prise à l'interprétation et au doute, même si cette carence est peu à peu comblée par les lignes directrices publiées par le groupe de travail « Article 29 ». En revanche, il ressort clairement du RGPD que le fait de se doter d'un DPO ne permettra pas, à lui seul, de démontrer le respect au RGPD. Le DPO est certes un expert, un guide, qui permet de faciliter la mise en œuvre du RGPD, mais il n'est pas un bouc émissaire. Si le DPO a pour rôle de fournir des conseils sur les actions à prendre pour la bonne application d'une mesure spécifique, le responsable du traitement et le sous-traitant restent responsables de la décision finale. Toutefois, ils doivent être conscients qu'avec le RGPD, toute mauvaise décision ou tout non-respect des conseils donnés par le DPO les exposera désormais à de très lourdes conséquences financières.

Synthèse préparée par :
Alfredo Zallone

The Data Protection Officer (DPO)

PANELISTS

▪ *The Data Protection Officer (DPO) is one of the GDPR's most relevant innovations and one that raises quite a few questions for many organisations, since it is often unclear who this subject is, when it must be appointed and what its tasks and responsibilities are in connection to the correct implementation of the GDPR rules within the organisation's structure.*

▪ *The very core of the GDPR is the concept of accountability, which requires processors and controllers to have a substantial approach to privacy related matters, rather than a formal one. Controllers and processors will have to implement appropriate and effective measures and be able to demonstrate compliance of processing activities with the GDPR, taking into account all peculiar aspects of their structure and of the processing themselves. In fact, any processing is peculiar and may imply different risks for data subjects, which must be analysed and evaluated to take appropriate countermeasures.*

▪ *The DPO stands within this context as a subject that will help organisations in their efforts to limit and keep under control such risks. Clearly, for the particular role it plays, the DPO will necessarily need to be granted independence, it will need to have deep technical knowledge of the GDPR and of the organisation's internal structure and processing activities, in order to better understand the specific risks involved.*

▪ *The DPO Panel, thanks to the brilliant observations of its speakers, analysed the subject from two main points of view: a practical one, introduced by Mr Rastrelli, Chief of Safety and Protection Department of Intesa Sanpaolo Bank, and a more technical one, explained by Mr. Konstantakopoulos and Mr. Henrotte, both lawyers of the Lexing® Network, representing Greece and Belgium.*

▪ *Since all controllers and processors will have to analyse the risk of each processing activity carried out, the first and most practical approach depicted by Mr Rastrelli helped understand the several steps taken to decide how to organize the monitoring of all processing activities in a complex group of undertakings such as that of an international bank. Into this decision process, the bank has decided to appoint a different DPO for each legal entity of each country, coordinated by a group DPO that would oversee all main aspects of the GDPR implementation.*

▪ *In the second part of the Panel, Mr Konstantakopoulos analysed the problems and issues related to the position of the DPO, in relation to its involvement, resources, independence and conflict of interest. It is in fact quite difficult for organisations to understand how the DPO will operate, and how its independence requirement will be met from a practical point of view. The GDPR clearly states that the DPO will not receive any instruction regarding the execution of its tasks, that it will report directly to the highest management level and that he may not be penalised or dismissed for performing such tasks. Furthermore, the DPO will be provided with the resources necessary to carry out all of its tasks. Notwithstanding such provisions, it appears that independence will be hard to reach from a practical point of view, since a DPO market will*

Fabio Rastrelli
Chief Compliance Officer
Banca Intesa (Milano, Italy)

Jean-François Henrotte
Lexing Belgium
belgium@lexing.network

Theodore Konstantakopoulos
Lexing Greece
greece@lexing.network

Moderator:

Alfredo Zallone
Lexing Italy
italy@lexing.network

flourish and, therefore, I will be possible to find a more accommodating DPO.

▪ *Mr Henrotte, taking into account these considerations, has reported three questions that he had received from his clients. One of those related to the concept of liability for the decisions and observations of the DPO which, as we know, will entirely fall on the controllers and processors. This will be one of the main incentives for them to follow the DPO's advice: they will be the ones taking responsibility. Subsequently he explained how the DPO will have to manage confidential information, and what kind of contractual warranties will be needed in order to "protect" his independence and himself from a premature dismissal. As we know, there are no civil sanctions for controllers or processors who remove DPOs from their position for executing their tasks, and to avoid the risk of subjugation to the management for fear of removal, a penalty clause in their appointment agreement may help mitigate such risk.*

▪ *As the Panel has pointed out several times, the GDPR is far from being the perfect regulation, and leaves a lot of room for interpretation and doubt, which is being slowly filled by the WP29 guidelines. What clearly emerges though is that organisations, even by appointing a DPO, will not be able to demonstrate compliance. The DPO is merely a facilitator of the implementation of the GDPR, an expert, a guide, but not a scape goat to which all compliance can be delegated. The DPO will simply give advice on what the correct way of implementing a specific measure is, while the controller and the processor will remain liable for taking the final decision. Only this time the consequences for taking the wrong one or for not following the DPO's advice, may be financially very serious.*

Summary prepared by
Alfredo Zallone

Welcome and introduction by Alain Bensoussan (France)

Keynote Speech: the GDPR by Giovanni Buttarelli, European Data Protection Supervisor (EDPS)

The Lexing Network by Frédéric Forster (France)

Privacy by design by Daniel Preiskel (UK), Sébastien Fanti (Switzerland), Françoise Gilbert (USA) & Marc Mossé (Microsoft)

The DPO by Jean-François Henrotte (Belgium), Alfredo Zallone (Italy) & Theodore Konstantakopoulos (Greece)

The role of the DPO by Fabio Rastrelli, Chief Compliance Officer of Banca Intesa

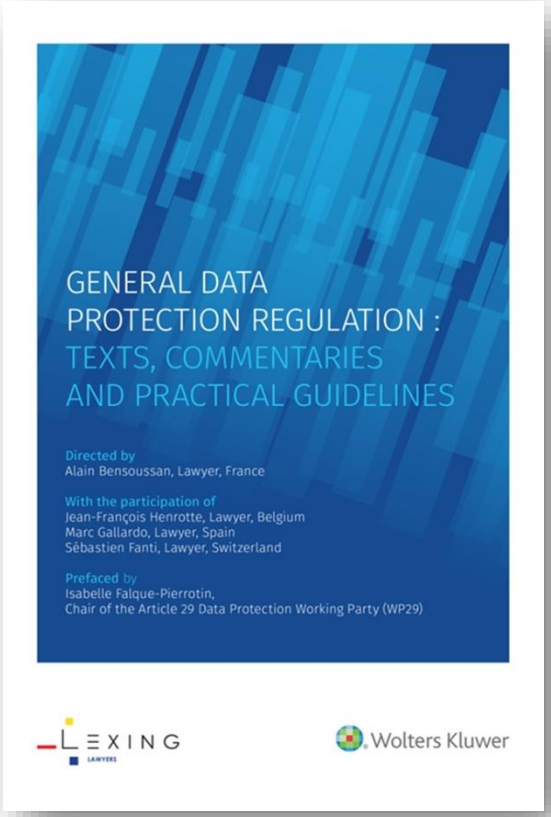
Data Transfer Issues by Gabriel Lizama (Costa Rica), Jun Yang (China), Koki Tada (Japan), Yassine Younsi (Tunisia) & Francesco Cajani (Procuratore della Repubblica – Milano)

Accountability, organisation & sanctions by João P. Alves Pereira (Portugal) & Roberto De Simone, Legal Adviser at SKY Italy

Take Home Points, Next Steps and Conclusion by Raffaele Zallone (Italy)

The Lexing team in Milan (Italy), at the GDPR conference organized by Lexing Italy (Studio Legal Zallone).
The next Lexing annual public conference will take place in Paris (France) in June 2018 and be organized by Lexing France (Lexing Alain Bensoussan Avocats). Mark your calendar!

LEXING - PUBLICATIONS



***Wolters Kluwer* (2017)**

Texte fondamental, le Règlement européen 2016/679 du 27 avril 2016, dit « RGPD », va bouleverser les règles du jeu du monde de la data et l'environnement numérique des entreprises.

Cet ouvrage propose aux lecteurs un commentaire, article par article, du RGPD afin d'en faciliter la mise en œuvre.

Sous la direction d'Alain Bensoussan (Lexing France) et avec la participation de Jean-François Henrotte (Lexing Belgique), Marc Gallardo (Lexing Espagne) et Sébastien Fanti (Lexing Suisse), il est préfacé par Isabelle Falque-Pierrotin, Présidente Groupe de travail « Article 29 » (G29).

The European Regulation 2016/679 of 27 April 2016, known as "GDPR", is a landmark that will disrupt the rules in the world of data and the digital business environment.

This practical guide, which provides an article-by-article commentary of the GDPR, will help you prepare and get ahead.

Directed by Alain Bensoussan, (Lexing France), with the participation of Jean-François Henrotte (Lexing Belgium), Marc Gallardo (Lexing Spain) and Sébastien Fanti (Lexing Switzerland), it is prefaced by Isabelle Falque-Pierrotin, Chair of the Article 29 Data Protection Working Party (WP29).

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
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
Guatemala *Guatemala*	Morales, Redondo & Vargas	Ada Lissette Redondo Aguilera	+(502)2331-8057	guatemala@lexing.network
Inde *India*	Poovayya and Co	Siddhartha George	+91 80 4115 6777	india@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 : Data Protection©Mathias Rosenthal_Fotolia