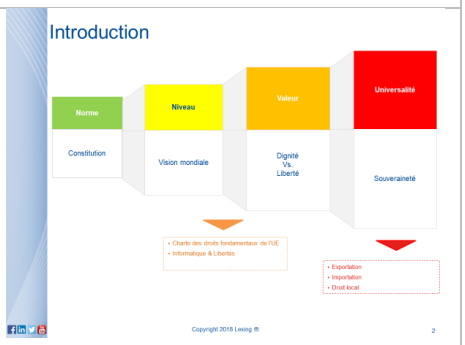
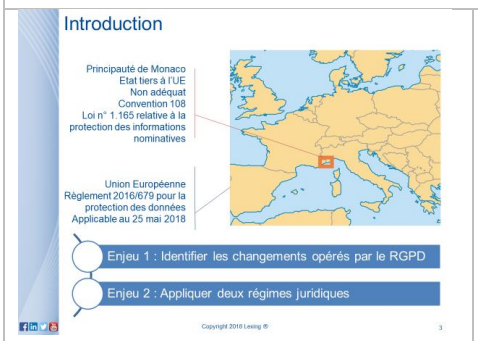
Les enjeux du RGPD au sein de la Principauté de Monaco

Synthèse de la présentation du 7 mai 2018 aux acteurs du secteur privé

A l'initiative du Gouvernement Princier, une journée d'information sur la mise en place de la nouvelle règlementation de l'Union Européenne en matière de protection des données personnelles s'est tenue le 7 mai 2018. Cette présentation du Règlement Général sur la Protection des Données (RGPD) 2016/679, de ses enjeux et de ses impacts pour Monaco par Me Alain Bensoussan, avocat spécialisé en droit des nouvelles technologies, a pour objectif de sensibiliser les acteurs économiques de la Principauté.

Le RGPD est un texte de niveau constitutionnel. Il propose le plus haut niveau de protection au monde en matière de données à caractère personnel.
Il se place sur le terrain des valeurs et de l'universalité.
La philosophie du RGPD se base sur le concept de dignité et s'oppose ainsi dans sa conception au principe de liberté du 1er amendement américain. Le principe n'est pas celui de la liberté de faire mais au contraire celui de l'anonymat et de l'interdiction de traiter des données à caractère personnel sauf à respecter les dispositions réglementaires en vigueur.

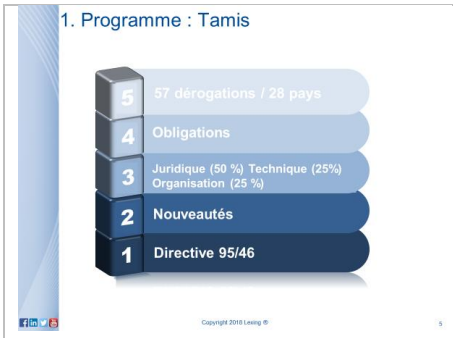




La Principauté de Monaco est un pays tiers à l'Union européenne. Il n'a pas bénéficié d'une décision d'adéquation sous l'égide de la directive 95/46/CE. Il est membre de la Convention 108 pour la protection des données à caractère personnel et dispose d'un cadre légal proche des dispositions européennes et françaises en matière de protection des données à caractère personnel (la loi 1.165 relative à la protection des informations nominatives).
L'avènement du RGPD et son applicabilité au 25 mai 2018 nécessitent pour les acteurs privés et publics monégasques de s'interroger sur les changements opérés par le RGPD et leur champ d'application. Le régime de la loi monégasque 1.165 et le régime du RGPD vont coexister jusqu'à l'adoption d'une nouvelle loi monégasque.

La présentation propose :

- de passer le RGPD au tamis afin d'en définir les contours ;
- d'identifier les principes fondamentaux et les exigences du RGPD et notamment les nouveautés ;
- de définir les droits des personnes et les risques financiers du non respect des dispositions du RGPD ;
- d'analyser le champ d'application du RGPD notamment au regard des activités des acteurs privés monégasques.



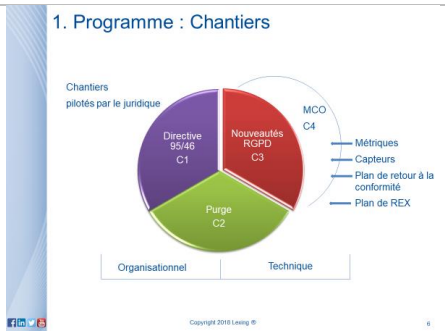
Le texte du RGPD :

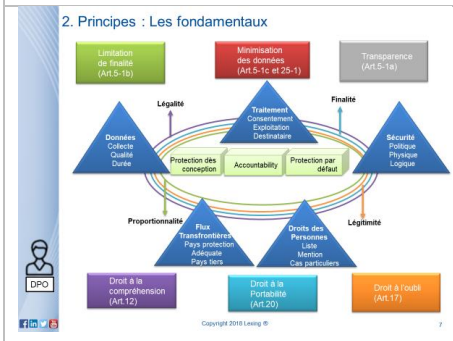
- reprend un grand nombre de principes et dispositions de la directive 95/46/CE ;
- intègre des nouveautés et notamment un changement notable qui anime toute la philosophie du RGPD : celui de la responsabilisation des acteurs. Les principes de protection dès la conception, de protection par défaut et d'accountability participent de ce renversement d'approche ;
- le texte du RGPD pose certes un certain nombre d'obligations juridiques mais pose également des recommandations et des obligations en termes techniques et organisationnels ;
- le RGPD c'est 99 articles, 193 considérants et 416 obligations ;
- le texte est parfois appelé « Règlement sui generis » car, si en tant que règlement il est d'application directe au sein des Etats membres, le texte propose 57 dérogations possibles dont chacun des 28 Etats membres peut se saisir pour adapter le règlement à ses spécificités nationales.

Un chantier de mise en conformité doit être piloté par le juridique ; il nécessite également des chantiers techniques et organisationnels. Les chantiers de mise en conformité impliquent de vérifier la conformité à la directive 95/46/CE, d'implémenter les nouveaux concepts, obligations, outils du RGPD et de réaliser une purge des données, bien souvent négligée.

Un processus de mise en conformité est à distinguer d'un principe de légalité :

- le principe de légalité est statique et binaire : soit on respecte la loi, soit on est dans l'illégalité ;
- le processus de conformité est quant à lui dynamique et continu. Il nécessite de mettre en place des indicateurs de suivi, des éléments de mesures, de procéder à des retours d'expérience afin de définir des plans de retour à la conformité en cas d'écart.





Les principes fondamentaux définis par la directive 95/46/CE restent pleinement applicables et sont réaffirmés à l'article 5 du RGPD : principes de légalité, de finalité, de proportionnalité et de légitimité.

Le traitement des données à caractère personnel doit s'opérer conformément à ces principes. Les personnes concernées doivent être informées de leurs droits ; les données doivent être conservées et traitées de manière sécurisée. Le texte encadre également les flux transfrontières de données.

Le RGPD pose de nouveaux concepts, socle de la nouvelle philosophie de la matière : les principes de protection dès la conception, de protection par défaut et d'accountability.

Le RGPD crée également de nouveaux droits : le droit à la compréhension, le droit à la portabilité, le droit à l'oubli, la transparence, le principe de limitation de finalité et, le plus important, le principe de minimisation des données.

Les exigences clés du RGPD qu'il convient d'appliquer à chaque traitement de données à caractère personnel sont les suivantes :

- la licéité : il convient de vérifier que le traitement est réalisé sur une base licite. L'article 6 du RGPD liste 6 justifications : ainsi un traitement est licite s'il est opéré : avec le consentement de la personne, pour l'exécution d'un contrat, dans le respect d'une obligation légale, pour la sauvegarde des intérêts vitaux de la personne, pour l'exécution d'une mission de service public, aux fins des intérêts légitimes du responsable de traitement.
- la loyauté : les données doivent être traitées conformément aux informations transmises à la personne concernée et à partir desquelles elle a consenti au traitement.
- la transparence : la transparence impose de transmettre aux personnes concernées les informations nécessaires sur les traitements opérés et notamment les finalités ;
- la définition des finalités : un traitement doit répondre à des finalités déterminées, explicites et légitimes ;
- la minimisation des données : les données collectées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».
- l'exactitude des données : les données doivent être « exactes et, si nécessaire, tenues à jour ». Le responsable de traitement doit s'assurer des processus de mise à jour et de suppression des données.
- la sécurité : le responsable du traitement doit garantir la sécurité des données traitées et mettre en œuvre les mesures techniques et organisationnelles appropriées.

Pour réaliser cette démarche de conformité et respecter les exigences clés, le RGPD propose un certain nombre d'outils ou de fonctions :

- le Délégué à la protection des données « DPD » ou Data Protection Officer « DPO » (articles 37 à 39 RGPD) : homme clé de la conformité, il est chargé d'informer, de conseiller et de former le responsable du traitement ainsi que ses employés ;
- l'analyse d'impact (articles 35 et 36 RGPD) : cette analyse est obligatoire lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ;
- le Registre (article 30 RGPD) : le RGPD supprime les formalités préalables (déclaration ou autorisation) et les remplace par la tenue d'un registre recensant tous les traitements d'une entité et des informations structurantes. Le RGPD fixe à 250 le nombre d'employés au-delà duquel le registre est obligatoire pour les entités mais les Etats disposent d'une marge d'appréciation ; sa tenue est toutefois fortement recommandée au regard du principe d'accountability pour les autres ;
- les mesures techniques et organisationnelles : l'expression est utilisée à plusieurs reprises dans le RGPD et impose au responsable de traitement et au sous-traitant de mettre en place des mesures appropriées pour garantir la sécurité, l'intégrité des données ainsi que la protection de la confidentialité. Anonymisation, pseudonymisation, chiffrement, gestion des habilitations, sécurité des accès sont des exemples de mesures.
- l'adhésion à un code de conduite (article 40 RGPD) et la démarche de certification (article 42 RGPD) peuvent servir d'éléments pour démontrer le respect des obligations incombant au responsable du traitement et pourront être prises en compte par l'autorité de contrôle en cas de procédure contentieuse.

Le RGPD est venu renforcer les droits des personnes déjà existant sous la directive 95/46/CE.
Les personnes concernées disposent ainsi sur leurs données de droits d'accès, de retrait, d'opposition à leur traitement.
Elles peuvent interroger le responsable de traitement pour faire valoir ces droits et disposer d'informations, sur l'existence d'un sous-traitant par exemple.
Le RGPD a introduit :

- le droit à l'oubli : chaque personne dispose du droit de supprimer numériquement les traces de son passé.
- Le droit à la portabilité : possibilité de transférer les données pour une gestion personnelle ou par l'intermédiaire d'un nouveau prestataire.

Chaque personne physique dispose par ces droits d'une plus grande maitrise de ses données et de leur traitement.

Le RGPD élève considérablement le niveau des sanctions en cas de non-respect des obligations et des principes posés par le texte.

Les amendes sont réparties en deux catégories en fonction de la nature des manquements :

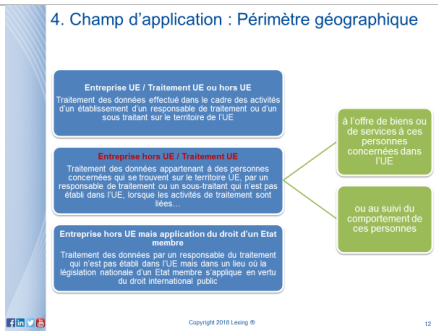
- maximum 10 000 000 d'euros ou 2 % du chiffre d'affaires mondial de l'exercice précédent ;
- maximum 20 000 000 d'euros ou 4 % du chiffre d'affaires mondial de l'exercice précédent.

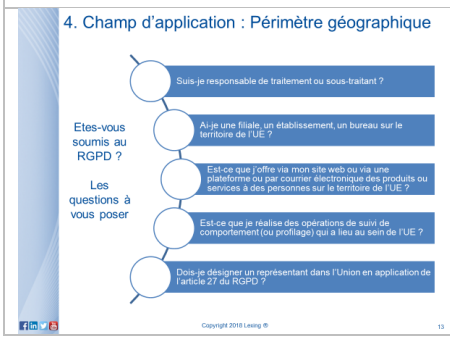
Sont également ouvertes les actions de groupe, ce qui risque d'élever les niveaux de sanction précédemment prononcés par les tribunaux, et les actions pénales contre le responsable de traitement.

Le RGPD s'applique directement à tous les traitements réalisés par un responsable de traitement ou un sous-traitant situé sur le territoire de l'UE.

LE RGPD s'applique également au responsable de traitement ou au sous-traitant situé dans un pays tiers (sur le territoire monégasque) et :

- soit offrant des biens ou services à des personnes situées sur le territoire de l'UE, qu'un paiement soit exigé ou non (considérant 23 RGPD)
- soit réalisant des traitements de profilage de personnes situées sur le territoire de l'UE.





Les acteurs monégasques sont invités à se poser un certain nombre de questions afin de vérifier s'ils sont soumis ou non au RGPD pour un ou plusieurs de leurs traitements.

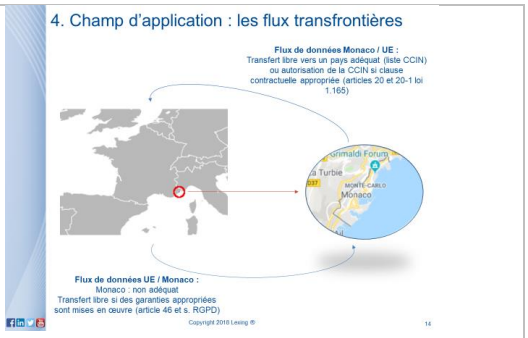
Dans l'hypothèse où ils sont soumis à l'application du RGPD, l'article 27 leur impose de désigner une personne physique ou une personne morale chargée de les représenter et d'échanger avec les autorités de contrôle au sein de l'Union européenne.

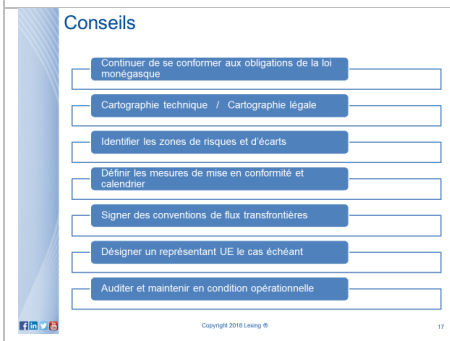
Les articles 44 et suivants du RGPD prévoient qu'un responsable de traitement ou un sous-traitant situé en UE ne peut transférer de données à caractère personnel dans un pays n'assurant pas un niveau de protection adéquat selon la Commission (décision d'adéquation) ou n'ayant pas mis en place des garanties appropriées telles que :

- les règles d'entreprise contraignantes ;
- les clauses types de protection des données ;
- le code de conduite ;
- le mécanisme de certification.

Les articles 20 et 20-1 de la loi 1.165 relative à la protection des informations nominatives prévoient des dispositions similaires pour tout transfert d'informations nominatives hors de la Principauté.

Les acteurs monégasques doivent se doter de dispositions contractuelles sécurisantes pour pouvoir échanger des données à caractère personnel avec des personnes où qu'elles se situent.





Au regard de l'impact et des enjeux du RGPD, les conseils formulés aux acteurs monégasques sont les suivants.

Il convient en premier lieu de continuer de se conformer aux dispositions légales monégasques relatives aux informations nominatives et notamment continuer de procéder aux déclarations de ses traitements.

Pour les acteurs concernés, il convient d'engager une démarche de mise en conformité au RGPD. Cette démarche nécessite avant toute action :

- de réaliser une cartographie technique des systèmes d'information (identifier les applications et les traitements opérés) et vérifier leur conformité légale au regard du RGPD ;
- d'identifier les zones d'écart et de risques ;
- de définir les mesures de mises en conformité et le calendrier d'implémentation des actions ;
- de vérifier ses contrats et signer des conventions de flux transfrontières ;
- de désigner un représentant sur le territoire de l'UE.

Il est enfin nécessaire de définir des indicateurs et d'auditer régulièrement les mesures afin de vérifier leur maintien en condition opérationnelle.