KPMG GLD & Associés Monaco

LOI 1.565 : sécurité des données et notification des violations

■ **ADVISORY** ■ CYBER

■ *Newsletter N°4*

Loi 1.565 : Quelles sont les nouvelles obligations en matière de sécurité des données et de notification des violations de données ?

La Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles bouleverse les obligations des responsables de traitement. De façon générale, la grande révolution de ce texte est la suivante : **le responsable de traitement** est maintenant placé « au cœur de sa propre conformité ».

C'est-à-dire qu'il lui incombe pleinement **s'assurer de son respect du texte** : Les autorisations délivrées par une autorité de protection des données valant conformité des traitements, c'est (presque) fini.

De nombreux articles sont déjà publiés sur le sujet, et sur les changements qui en découlent en termes de documentation pour les responsables de traitement. Nous n'y reviendrons pas. En revanche, deux obligations font l'objet de notre article :

1. **Obligations en matière de sécurité et de confidentialité** : Les responsables de traitement doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque.
2. **Notification des violations de données à caractère personnel** : En cas de violation de données personnelles, le responsable de traitement doit informer l'autorité compétente de protection des données ainsi que, dans certains cas, les personnes concernées.

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

Ces deux obligations méritent une attention particulière, notamment en ce qui concerne l**a sécurité des traitements** (Art. 31 de la Loi 1.565) : aucun texte ne précise clairement quelle sécurité est appropriée pour chaque traitement. Mais alors, **comment trouver la sécurité adéquate pour un traitement ?**

Dans le cas de la violation de données (Art. 32 et suivants de la Loi 1.565), le processus est bien défini. Mais **quelles sont les obligations liées à la violation de données et comment la prévenir ?**

Il est crucial pour les responsables de traitement opérant à Monaco de respecter ces obligations afin de garantir une protection adéquate des données personnelles et d'éviter des sanctions potentielles, bien plus sévères que sous le régime de la CCIN.

Comment trouver la sécurité adéquate pour un traitement de données personnelles ?

La notion de sécurité pour un traitement repose sur 3 « besoins de sécurité » :

- La confidentialité : la donnée doit être révélée seulement à certaines personnes ;
- L'intégrité : la donnée doit être exacte, non modifiée lors d'un transfert par exemple ;
- La disponibilité : la donnée doit être disponible, accessible au moment nécessaire.

Chaque traitement de données a des besoins spécifiques qui doivent être adaptés en conséquence. Par exemple : un traitement concernant « le calcul et le versement des salaires des collaborateurs de la société X » nécessite intuitivement un fort besoin de confidentialité et d'intégrité : on veut éviter d'en divulguer les montants (confidentialité), et les montants virés doivent être exacts (intégrité).

Il est recommandé de mettre en place des mesures de sécurité pour garantir la confidentialité (limitation des accès, chiffrement des données au repos) et des mesures organisationnelles pour assurer l'intégrité (automatisation des calculs pour minimiser les erreurs, validation des salaires par deux personnes, utilisation d'un logiciel fiable pour l'envoi des ordres de banque).

Il ne faut pas oublier qu'une sécurité adaptée doit répondre aux critères suivants :

- « À l'état de l'art » : elle repose sur des moyens éprouvés actuels (et non trop vieux),
- « Dynamique » : elle évolue et elle est réexaminée en fonction des nouvelles menaces ;
- « En profondeur » : elle repose sur plusieurs couches de sécurité complémentaires et pas une seule sécurité.

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

Enfin, chaque mesure de sécurité a un coût et doit être proportionnée au traitement et aux données qu'elle protège.

Aussi, il est nécessaire de bien penser au **risque pour les personnes** lors de la mise en œuvre d'un traitement, et se faire accompagner par des professionnels de la cybersécurité reste pertinent pour obtenir une sécurité adéquate au coût le plus raisonnable.

Mais souvenez-vous aussi que **le risque diminue à la source lorsqu'on s'assure de ne collecter que les données nécessaires à son besoin** : par exemple en prenant une tranche d'âge au lieu d'une date d'anniversaire pour un traitement marketing.

Quelles sont les obligations liées à la violation de données et comment la prévenir ?

Les **sources de violation de données** sont variées : elles peuvent être dues à **des accidents** (incendie de salle serveur entraînant une indisponibilité), **des erreurs** (une secrétaire envoie un mail personnel au mauvais destinataire entraînant une divulgation de données), ou **des actes de malveillance** (un pirate vole et chiffre les données de l'entreprise, entraînant une indisponibilité, une perte d'intégrité et une perte de confidentialité générale).

Quels sont d'abord les devoirs du responsable de traitement ? Tout d'abord, établir **un registre des violations de données**. C'est souvent un outil de conformité oublié. Mais l'art. 32 précise bien que les responsables de traitement documentent toutes les violations de données à caractère personnel.

Quelle que soit la cause de la violation de données personnelles, il est nécessaire de documenter l'incident en interne :

- La **nature** supposée de la violation ;
- Les **conséquences probables** de la violation de données ;
- Le **nombre approximatif** de personnes concernées ;
- Les **mesures** pour éviter que l'incident se reproduise ou pour atténuer ses conséquences négatives ;
- Les catégories et le nombre approximatif **de données** concernées.

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

Mais, suivant le risque estimé pour les personnes concernées, il ne suffit pas de tenir un registre interne, des notifications sont prévues :

Risque pour les personnes concernées :	Aucun	Non élevé	Elevé
Documentation sous forme d'un registre interne des différentes violations dont il est victime	✓	✓	✓
Notification à l'APDP sous 72h		✓	✓
Informations des personnes concernées, dans les meilleurs délais hors cas particuliers			✓

Il y a quand même 3 exceptions à l'information des personnes concernées :

1. **Les efforts sont disproportionnés** pour informer individuellement toutes les personnes concernées. Attention, dans ce cas, le Responsable de traitement doit lancer une communication publique !
2. **Mise en place de mesures à postériori**. C'est le cas où l'entreprise a mis en place, après la violation de données, des mesures empêchant le risque élevé de survenir. Par exemple : Des accès à des personnes non autorisées sur une base de données sensibles ont été détectés et corrigés.
3. **Mesures de protection efficaces**. Le responsable de traitement a mis en œuvre des mesures techniques et organisationnelles de protection qui rendent les données incompréhensibles pour toute personne non autorisée à y accéder.

Il est clair que la sécurité informatique joue un rôle crucial dans la prévention des violations de données, mais ce n'est pas le seul aspect à considérer. En effet, sur les deux derniers points évoqués, de bonnes pratiques de sécurité informatique peuvent également entrer en jeu.

Reprenons notre exemple : Des accès à des personnes non autorisées sur une base de données sensibles ont été détectés et corrigés. Comment faire **la preuve** que la mesure a empêché une violation de se produire ?

Cela ne sera possible que si les accès à cette base sont journalisés, autrement dit **qu'on en possède les « logs »** et que ces logs sont stockés dans une zone réseau empêchant leur falsification par exemple.

Ainsi, le responsable pourra facilement documenter son incident en montrant que les accès, s'ils ont été attribués, n'ont pas été utilisés avant que la correction ait eu lieu.

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

Concernant notre dernier point, imaginons qu'un **site internet soit piraté** et que les accès, mots de passe et cartes de crédit soient volés. Là encore, **une bonne hygiène informatique peut éviter la notification aux personnes concernées** : le chiffrement et le hachage des données dans la base de données, en utilisant des algorithmes sûrs et à l'état de l'art, sont reconnus suffisamment robustes comme mesures de sécurité efficaces.

Ainsi, **on comprend que les obligations pesant sur les responsables de traitements sont renforcées avec la Loi 1.565 et que la complexité de la mise en conformité est accrue par le renvoi des réflexions techniques sur le responsable de traitement**.

S'il était déjà question de sécurité lorsqu'on déclarait un traitement à la CCIN, aujourd'hui les peines sont plus sévères. Les mesures comme l'obligation de déclaration en cas de violation de données, devraient aussi inciter les responsables de traitement à être plus attentifs dans leurs pratiques pour préserver leur image.

Le sujet de la sécurité informatique est un domaine technique pointu, qui peut nécessiter un accompagnement pour bénéficier d'une posture confortable vis-à-vis du régulateur « APDP » à Monaco.

Comme d'autres décisions dans la vie d'un entrepreneur, savoir s'entourer et s'informer auprès de sources sûres sera donc primordial.

Auteurs

Clément MAILLIOUX

Directeur • Advisory • KPMG Monaco

cmaillioux@kpmg.mc

Sabina DEBUSSY

Directeur Associé • Advisory • KPMG Monaco

sdebussy@kpmg.mc

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.

Contactez-nous

Bettina RAGAZZONI
Associé
bragazzoni@kpmg.mc

Stéphane GARINO
Associé Principal
sgarino@kpmg.mc

Xavier CARPINELLI
Directeur Associé Expertise
xaviercarpinelli@kpmg.mc

Anne Marie FELDEN
Directeur Associé Audit
afelden@kpmg.mc

Sylvie ROTI
Directeur Associé Expertise
sroti@kpmg.mc

Sabina DEBUSSY
Directeur Associé Advisory
sdebussy@kpmg.mc

Patrice DARMON
Directeur Associé Expertise
pdarmon@kpmg.mc

Mélanie LE MOIGN
Directeur Associé Audit
mlemoign@kpmg.mc

Cécile BOZANO-BODIN
Directeur Associé Advisory
cbozanobodin@kpmg.mc

Alain CHARPENTIER
Directeur Associé Audit
acharpentier@kpmg.mc

KPMG GLD & Associés Monaco

2, rue de la Lüjerneta • "Athos Palace" • 98000, Monaco

mc-news@kpmg.mc
www.KPMG.mc
@KPMG_Monaco
+377 977 777 00
@kpmg-monaco
@KPMGMonaco

Les informations contenues dans ce document sont d'ordre général et ne sont pas destinées à traiter les particularités d'une personne ou d'une entité. Bien que nous fassions tout notre possible pour fournir des informations exactes et appropriées, nous ne pouvons garantir que ces informations seront toujours exactes à une date ultérieure. Elles ne peuvent ni ne doivent servir de support à des décisions sans validation par les professionnels ad hoc. KPMG International ne propose pas de services aux clients. Aucun cabinet membre n'a le droit d'engager KPMG International ou les autres cabinets membres vis-à-vis des tiers. KPMG International n'a le droit d'engager aucun cabinet membre.

Déclaration de Confidentialité | Mentions légales

© KPMG GLD et Associés S.A.M., une société anonyme monégasque d'expertise comptable et membre du réseau global KPMG constitué de cabinets indépendants adhérents de KPMG International Limited ("KPMG International"), une société privée à responsabilité limitée par garanties de droit anglais. Tous droits réservés.