Décision de sanction en date du 18 juillet 2017

du Président de la Commission de Contrôle des Informations Nominatives

à l'encontre de *[l'établissement]*

Avertissement suite à investigation et publication de la sanction

Rappel des faits :

Par délibération n° 2016-83 du 16 juin 2016 la Commission de Contrôle des Informations Nominatives a décidé de mener une mission d'investigation au sein des locaux de *[l'établissement],* à la suite de la divulgation non autorisée d'informations nominatives relatives aux Agents par le biais de l'utilisation frauduleuse de la messagerie électronique de l'établissement.

Cette mission d'investigation a été prorogée par délibérations n° 2016-112 du 20 juillet 2016 et n° 2016-138 du 19 octobre 2016.

Les opérations de contrôle sur place, effectuées les 21 juin, 15 juillet, 15, 16 18 21, 24, 25 novembre 2016 et les 9, 10 et 13 janvier 2017, ont mis en exergue plusieurs manquements aux dispositions de la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée.

Conformément à l'article 18 alinéa 8 de la Loi n° 1.165, les procès-verbaux des constatations, vérifications et visites ont été dressés contradictoirement.

En application de l'article 19 de la Loi n° 1.165 susmentionnée, le rapport détaillant les irrégularités relevées lors de ces opérations de contrôle a été notifié à *[l'établissement]* en date du 30 mars 2017, afin qu'il puisse faire part de ses observations sur celui-ci dans un délai d'un mois.

Ce dernier n'a pas produit de commentaire écrit sur le rapport, s'attachant à mettre d'ores et déjà en œuvre un plan d'action correctif de certains manquements constatés.

Motifs de la sanction :

- Sur la mise en œuvre des traitements automatisés d'informations nominatives :

Il a été relevé l'exploitation de traitements automatisés d'informations nominatives n'ayant pas été soumis préalablement à la CCIN.

Ceci constitue une non-conformité à l'article 7 de la Loi n° 1.165, susmentionnée, aux termes duquel *« la mise en œuvre de traitements automatisées d'informations nominatives par des responsables de traitements, personnes morales de droit public, autorités publiques, organismes de droit privé investis d'une mission*

d'intérêt général ou concessionnaires d'un service public portés sur une liste établie par arrêté ministériel, est décidée par les autorités ou par les organes compétents après avis motivé de la Commission de Contrôle des Informations Nominatives.

Cette décision et l'avis motivé qui l'accompagne font l'objet d'une publication au Journal de Monaco dans les conditions fixées par ordonnance souveraine. En ce qui concerne les traitements visés à l'article 11, ne donnent lieu à publication que le sens de l'avis de la commission et de la décision de l'autorité ou de l'organe compétent.

Si l'avis de la Commission est défavorable, l'autorité ou l'organisme compétent ne peut mettre en œuvre le traitement qu'après y avoir été autorisé par arrêté motivé du Ministre d'Etat ou du directeur des services judiciaires. »

- Sur la durée de conservation des informations nominatives :

Il a été relevé des durées de conservation des informations nominatives excessives et dans certains cas illimitées.

Ceci constitue une non-conformité à l'article 10.1 de la Loi n° 1.165, susmentionnée, aux termes duquel *« Les informations nominatives doivent être (…) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées ou pour laquelle elles sont traitées ultérieurement ».*

- Sur la sécurité et la confidentialité des informations nominatives :

Il a été relevé plusieurs non conformités à l'article 17 de la Loi n° 1.165, susmentionnée, aux termes duquel *« Le responsa*ble *du traitement ou son représentant est tenu de prévoir des mesures techniques et d'organisation appropriées pour protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions d'informations dans un réseau, ainsi que contre toute autre forme de traitement illicite.*

Les mesures mises en œuvre doivent assurer un niveau de sécurité adéquat au regard des risques présentés par le traitement et de la nature des données à protéger.

Lorsque le responsable du traitement ou son représentant a recours aux services d'un ou plusieurs prestataires, il doit s'assurer que ces derniers sont en mesure de satisfaire aux obligations prescrites aux deux précédents alinéas.

La réalisation de traitements par un prestataire doit être régie par un contrat écrit entre le prestataire et le responsable du traitement ou son représentant qui stipule notamment que le prestataire et les membres de son personnel n'agissent que sur la seule instruction du responsable du traitement ou de son représentant et que les obligations visées aux deux premiers alinéas du présent article lui incombent également. »

Il s'agit de dysfonctionnements relatifs à la sécurisation du système d'information *[de l'établissement]* et à la mise en œuvre des règles de sécurité destinées à préserver l'intégrité et la confidentialité des données nominatives.

Ces manquements se traduisent par une sécurité logique comportant des insuffisances (défaut de suivi des habilitations, traçabilité des accès non généralisée,…) et par la non application de règles de sécurité adéquates (absence de gestion des mots de passe : fréquence de changement, complexité, répudiation en cas d'échec ; existence de comptes partagés ; déploiement partiel des mesures de verrouillage automatique de sessions ; …).

Par ailleurs les contrats conclus avec les prestataires ne comportent pas de clauses spécifiques relatives à la préservation de la sécurité et de la confidentialité des données ainsi qu'à l'encadrement de leurs interventions.

Décision :

Au regard des éléments ci-dessus développés, un avertissement est justifié. Néanmoins il a été pris en compte la transparence dont a fait preuve *[l'établissement]* lors des opérations d'investigation, ainsi que la mise en œuvre de mesures correctives rapides concernant les dysfonctionnements les plus urgents.

De plus *[l'établissement]* a fait procéder très rapidement de sa propre initiative à un audit de sécurité de son système d'information.

Cependant la mise à niveau de celui-ci au regard des standards exigés en la matière n'est pas encore entièrement effectuée.

Aussi un plan d'action détaillant et planifiant la mise en œuvre des mesures correctives qui seront apportées devra être transmis à la Commission de Contrôle des Informations Nominatives dans un délai de deux mois.

Enfin, eu égard au nombre de personnes concernées par ces irrégularités, à l'importance de certaines de ces non conformités et à la nature de l'activité de cet établissement, la présente sanction sera rendue publique puis anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

Les mesures de publicité de la présente sanction peuvent faire l'objet d'un recours devant le Président du Tribunal de première instance, dans les formes et conditions prévues à l'article 19 alinéa 7 de la Loi n° 1.165, susvisée.

Le Président

Guy MAGNAN