

Délibération n° 2019-027 du 20 février 2019

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Gestion des accès aux locaux et des horaires par badge magnétique* »

présenté par Union Bancaire Privée – Succursale de Monaco

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu la délibération n° 2010-43 du 15 novembre 2010 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs de contrôle d'accès sur le lieu de travail mis en œuvre par les personnes physiques ou morales de droit privé ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'autorisation déposée par Union Bancaire Privée – Succursale de Monaco le 25 octobre 2018 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Système de badge permettant contrôle d'accès et gestion des horaires* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 21 décembre 2018, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 20 février 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Union Bancaire Privée (UBP) est la succursale à Monaco de UBP SA, établissement bancaire suisse (Genève), immatriculée au répertoire du Commerce et de l'Industrie sous le numéro 14S06257, qui a pour activité « *la réalisation de toutes opérations de banque ou connexes telles que définies par la loi bancaire applicable (...)* ».

Afin d'assurer la sécurité des biens et des personnes au sein de ses locaux et la confidentialité des données mais aussi afin de gérer les horaires et temps de présence de ses employés, cette société souhaite installer un système de contrôle des accès par badges magnétiques.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance, il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le responsable de traitement indique que le traitement a pour finalité « *Système de badge permettant contrôle d'accès et gestion des horaires* ».

Les personnes concernées sont les employés et les tiers. A cet égard, la Commission constate à la lecture du dossier que les tiers englobent les auditeurs externes ainsi que les prestataires/sous-traitants permanents.

Enfin, les fonctionnalités sont les suivantes :

- assurer la sécurité des personnes et des biens par ségrégation des accès entre les clients, le personnel et les intervenants extérieurs ;
- assurer la sécurité des personnes et des biens en contrôlant les accès aux locaux identifiés comme sensibles bénéficiant d'une circulation limitée ;
- gérer les habilitations d'accès aux personnes autorisées ;
- désactiver les badges perdus/volés ;
- permettre la constitution de preuves en cas d'infraction ;
- gérer les horaires et les temps de présence des employés ;
- permettre à l'équipe Sécurité Incendie de savoir qui serait sur le site sinistré en cas de survenance d'aléas et non au point de RDV évacuation.

La Commission rappelle toutefois que tout traitement d'informations nominatives doit avoir une finalité « *déterminée, explicite et légitime* » aux termes de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

En l'espèce, la finalité du présent traitement doit être plus explicite c'est-à-dire être claire et précise pour les personnes concernées en indiquant que le contrôle des accès s'effectue par le biais de badges magnétiques.

Par conséquent, elle modifie la finalité comme suit : « *Gestion des accès aux locaux et des horaires par badge magnétique* ».

II. Sur la licéité et la justification du traitement

Le traitement est justifié par la réalisation d'un intérêt légitime poursuivi par le responsable du traitement, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission constate ainsi que ce système va permettre d'assurer « *la protection des personnes et des biens* » ainsi que « *la confidentialité des données détenues grâce à une restriction d'accès aux locaux aux seules personnes dûment habilitées* ».

Elle relève par ailleurs que ledit système va également permettre de gérer « *les horaires et les temps de présence des employés dans une optique d'offrir plus de flexibilité aux employés dans la gestion de leur temps de travail* » et « *de connaître les heures supplémentaires effectuées afin de les intégrer aux données de paie ainsi que de permettre à l'équipe Sécurité Incendie de savoir qui serait sur le site sinistré en cas de survenance d'aléas et non au point de RDV évacuation* ».

Enfin, la Commission note que ledit traitement « *n'a pas pour objet de contrôler de manière inopportune les comportements et les habitudes des personnes concernées par le traitement* ».

Au vu de ce qui précède, elle considère que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Le responsable de traitement indique que les informations nominatives traitées sont :

- identité: nom et prénom du salarié, numéro de l'employé ;
- formation-diplômes/Vie professionnelle : service, fonction, plages horaires habituellement autorisées, zone d'accès autorisée ;
- données d'identification électronique : logs de connexion des personnels habilités à avoir accès aux informations et au traitement ;
- informations temporelles : date et heure de passage à une zone, nom et/ou numéro du point de passage ;
- badges : numéro de badge, date de délivrance et éventuellement code associé audit badge.

Le responsable de traitement indique que les informations relatives à l'identité des personnes, à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* » pour les employés et les contrats ou lettres de mission pour les prestataires permanents/sous-traitants.

En l'absence de précision, la Commission considère que les informations liées aux badges ont pour origine le système de contrôle d'accès par badge.

Le responsable de traitement indique par ailleurs que les informations relatives aux données d'identification électronique et aux informations temporelles ont pour origine le système de contrôle d'accès par badge.

La Commission considère ainsi que les informations collectées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

IV. Sur les droits des personnes concernées

➤ *Sur l'information préalable des personnes concernées*

Le responsable de traitement indique que l'information préalable des employés s'effectue par le biais d'une note de service affichée dans les locaux et par le biais d'une note de service spécifique.

Par ailleurs, l'information préalable des employés et des tiers (auditeurs externes, prestataires/sous-traitants) s'effectue également par le biais du formulaire de remise de clés et de badges.

A la lecture de ces documents, la Commission considère que les modalités d'information préalable des personnes sont conformes aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

➤ *Sur l'exercice du droit d'accès, de modification et de mise à jour*

Le responsable de traitement de traitement indique que le droit d'accès s'exerce sur place.

Il appert toutefois à la lecture du dossier que le droit d'accès des employés peut également s'exercer par voie postale auprès du Managing Director (Chief Operating Officer).

La Commission constate que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

V. Sur les destinataires et les personnes ayant accès au traitement

➤ *Sur les destinataires*

Les informations sont susceptibles d'être communiquées aux Autorités policières ou judiciaires légalement habilitées.

A cet égard, la Commission estime que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

Elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

La Commission considère donc que ces transmissions sont conformes aux exigences légales.

➤ *Sur les personnes ayant accès au traitement*

Les personnes habilitées à avoir accès au traitement sont :

- les membres du Service Sécurité de UBP Monaco et du Service Sécurité Groupe (UBP SA) suivant leurs habilitations : accès en inscription, modification, mise à jour et consultation concernant les informations liées à l'administration des accès physiques et accès en consultation uniquement des informations relatives à la badgeuse ;
- tous les employés de la banque : accès en inscription, modification, mise à jour et consultation concernant leurs propres horaires ;
- les responsables de service : accès en consultation des horaires des membres de leur service ;
- la direction : accès en consultation des horaires de tout le personnel ;

- les membres du service RH et du Groupe (UBP SA) : accès en inscription, modification, mise à jour et consultation concernant les informations liées à la badgeuse ;
- les personnes habilitées du service Administration Systèmes Groupe suivant leurs habilitations : accès en inscription, modification, mise à jour et consultation ;
- le service de Contrôle Interne : accès en consultation des informations des deux logiciels ;
- les prestataires : tous droits pour leurs opérations de maintenance, uniquement sous la supervision d'un personnel de la banque.

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

En ce qui concerne les prestataires, elle rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service. De plus, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

La Commission constate enfin qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 la liste nominative des personnes ayant accès au traitement est tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d'interconnexion et rapprochement avec deux traitements ayant respectivement pour finalité « *Gestion administrative des salariés* » et « *Gestion des fichiers de paie des personnels* » ; tous deux légalement mis en œuvre.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation particulière.

La Commission rappelle néanmoins que les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Elle rappelle également que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

Enfin, la Commission rappelle que la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations relatives à l'identité, à la formation, aux diplômes, à la vie professionnelle sont conservées 5 ans après la fin du contrat de travail pour les employés et 5 ans après la fin de la mission pour les auditeurs et prestataires/sous-traitants.

En l'absence de précision, la Commission considère que les informations liées aux badges sont également conservées 5 ans.

Le responsable de traitement indique par ailleurs que les données d'identification électronique sont conservées 1 an.

Enfin, les informations temporelles sont conservées 3 mois.

La Commission considère que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Gestion des accès aux locaux et des horaires par badge magnétique* ».

Constate que la liste nominative des personnes ayant accès au traitement est tenue à jour et précise qu'elle doit lui être communiquée à première réquisition.

Rappelle que :

- les Services de Police monégasque ne pourront avoir communication des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;
- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé ;
- la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

A la condition de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par Union Bancaire Privée – Succursale de Monaco du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des accès aux locaux et des horaires par badge magnétique* ».**

Le Président

Guy MAGNAN