Délibération n° 2023-144 du 18 octobre 2023

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 habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* »

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 la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financier ;

Vu la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée ;

Vu la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, modifiée ;

Vu l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée, susvisée ;

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 l'Ordonnance Souveraine n° 2.318 du 3 août 2009, modifiée, fixant les conditions d'application de la loi n° 1.362 du 3 août 2009, modifiée, relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, modifiée ;

Vu l'Arrêté Ministériel n° 2012.199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers ;

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 délibération n° 2017-206 du 20 décembre 2017 de la Commission de Contrôle des Informations Nominatives portant recommandation sur la gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au système d'information ;

Vu la demande d'autorisation déposée par Union Bancaire Privée – Succursale de Monaco le 21 juin 2023 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 18 août 2023, 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 18 octobre 2023 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 entre autres pour activité « *la réalisation de toutes opérations de banque ou connexes telles que définies par la loi bancaire applicable ».*

Afin de sécuriser l'accès à son système d'information (SI), cette société souhaite mettre en place un système d'habilitations.

Le traitement objet de la présente demande permet de surveiller les accès au système d'information, 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 traitement a pour finalité « *Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information ».*

Les personnes concernées sont les utilisateurs du Système d'Information.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

Dans le cadre de la gestion des habilitations :

- octroyer / délivrer aux utilisateurs du SI les moyens techniques et fonctionnels permettant de s'authentifier au système d'information afin de pouvoir exercer la fonction et les missions pour lesquelles ils ont été recrutés ;
- gérer les évolutions de droits, les mobilités internes et les départs ;
- mettre à jour les comptes systèmes dans le cadre de changements d'informations administratives (ex : changement de patronyme) ;

- permettre la réalisation de l'ensemble des tâches d'activation/ désactivation/suppression de comptes ;
- procéder à des revues de contrôles périodiques afin de s'assurer de la conformité des droits délivrés par rapport aux demandes et aux règles édictées en matière d'accès à l'information.

Dans le cadre de la supervision des accès aux applications :

- collecter des évènements systèmes (logs) permettant de tracer les accès des utilisateurs aux applications et données ;
- établir des alertes et/ou des rapports qui permettent de détecter tout risque de malveillance et de s'assurer de la cohérence des accès avec les habilitations délivrées ;
- établir des preuves en cas de litige avec tout utilisateur (employé, prestataire…).

Dans le cadre de la sécurité anti-virus :

- mettre en place des remontées d'alertes sur les risques d'intrusion ;
- établir des rapports (ex : audit de sécurité, détection de risques…).

La Commission constate ainsi que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le traitement est tout d'abord justifié par le respect d'une obligation légale, à savoir les obligations particulières de vigilance ainsi que de traçabilité des opérations effectuées imposées par :

- la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance Souveraine d'application ;
- la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, et son Ordonnance Souveraine d'application ;
- la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;
- l'Arrête Ministériel n° 2012-199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit-teneurs de comptes-conservateurs d'instruments financiers.

Le responsable de traitement indique par ailleurs que le traitement est également justifié par « *la réalisation d'un intérêt légitime poursuivi [par lui et qui] ne méconnait ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

A cet égard, la Commission prend acte que la procédure de surveillance ou de contrôle des habilitations informatiques permet :

- l'optimisation de l'accomplissement des missions de travail des employés ;
- la sécurité et le bon fonctionnement technique ou système informatique ;
- la préservation des intérêts économiques, commerciaux ou financiers du responsable de traitement ou de son représentant ;
- la prévention et la détection *a priori* et *a posteriori* de toute activité non-conforme ou illicite, par des utilisateurs.

Au vu de ce qui précède, la Commission considère donc 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

Les informations nominatives traitées sont :

- identité : nom, prénom et service de l'employé ou du prestataire ;
- données d'identification électronique : identifiants (login et mot de passe) de l'employé ou du prestataire ;
- informations temporelles : logs de connexion ;
- compte utilisateur : nom du compte, domaine du compte, groupe d'utilisateurs, type de droits.

Le responsable de traitement indique que les informations relatives à l'identité ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* ».

La Commission considère toutefois que concernant les prestataires externes ces informations ont pour origine le contrat de prestation de service.

Les données d'identification électronique et les informations concernant le compte utilisateur ont pour origine le Service Sécurité.

Enfin, les informations temporelles ont pour origine le système du présent traitement.

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*

L'information préalable des personnes concernées s'effectue par le biais d'une mention ou clause particulière intégrée dans un document remis à l'intéressé et par une mention particulière dans un document d'ordre général.

L'ensemble de ces documents n'ayant pas été joint à la demande, la Commission rappelle que l'information préalable des personnes concernées doit impérativement être effectuée conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Le responsable de traitement indique par ailleurs qu'il tient à la disposition desdites personnes « *la liste des traitements automatisés exploitant des informations nominatives* ».

La Commission estime toutefois qu'informer la personne concernée de la tenue à disposition d'une liste de traitements, qui nécessite de sa part une démarche active, n'est pas équivalent au fait de l'avertir, en ce que son abstention ne doit pas la priver d'être dûment informée. Aussi elle souligne que les modalités d'information des personnes concernées doivent être conforme à l'article 14 de la Loi n° 1.165.

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

Le droit d'accès s'exerce sur place auprès du Managing Director – Chief Operating Officer.

La Commission considère ainsi 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***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires dans le cadre de leurs missions légalement conférées.

La Commission considère ainsi que le Service d'Information et de Contrôle des Circuits Financiers (SICCFIN) (devenu Autorité Monégasque de Sécurité Financière (AMSF)) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires d'informations nominatives traitées.

Par ailleurs, elle estime que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ces autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

Sous ces conditions, elle considère donc que de telles 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 Monaco : inscription, modification, mise à jour et consultation ;
- les administrateurs fonctionnels & système du Service Informatique Groupe ou le Service Sécurité du Groupe et les collaborateurs du service informatique local : tous droits d'accès à ce traitement dans le strict cadre de l'accomplissement de leurs missions de contrôle, techniques et de maintenance système.

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

La Commission prend acte 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 rappelle que cette liste doit lui être communiquée à première réquisition.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique enfin que le présent traitement est interconnecté avec tous les traitements déjà mis en place ou à venir.

La Commission en prend acte.

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 la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Enfin, la Commission rappelle 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.

VIII. Sur les durées de conservation

Le responsable de traitement indique que les informations relatives à l'identité sont conservées 10 ans.

Les données d'identification électronique et les informations liées au compte utilisateur sont conservées toute la durée d'utilisation du SI par l'employé ou le prestataire.

Enfin, les informations temporelles sont conservées 1 an après la collecte d'information, à l'exception de la dernière date de connexion (et uniquement la plus récente) qui est conservée 2 ans « *afin de satisfaire aux demandes d'audit* » sur la gestion des révocations d'accès.

A cet égard, la Commission rappelle, conformément à sa délibération n° 2017-206 du 20 décembre 2017, que ces informations ne peuvent être conservées sous une forme permettant l'identification de la personne concernée que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour lesquelles elles ont été collectées.

Aussi, au regard des fonctionnalités du présent traitement, elle fixe la durée de conservation des informations relatives à l'identité à 3 mois maximum après le départ de l'utilisateur et celle des informations temporelles à 1 an maximum à compter de leur collecte.

Après en avoir délibéré, la Commission :

Rappelle que :

- l'information préalable des personnes concernées doit impérativement être effectuée conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- le SICCFIN et la CCAF peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires des informations du traitement ;

- les Autorités judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- la liste nominative des personnes ayant accès au traitement, tenue à jour, doit lui être communiquée à première réquisition ;

- 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 devra être chiffrée sur son support de réception.

Fixe la durée de conservation des informations relatives à l'identité à 3 mois maximum après le départ de l'utilisateur et celle des informations temporelles à 1 an maximum à compter de leur collecte.

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 habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* ».**

Le Président

Guy MAGNAN