DELIBERATION N° 2015-105 DU 18 NOVEMBRE 2015 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION A LA MISE EN ŒUVRE DU TRAITEMENT AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE « *GESTION ET SUPERVISION DE LA MESSAGERIE PROFESSIONNELLE* » PRESENTE PAR LA BANCA POPOLARE DI SONDRIO (SUISSE) S.A. REPRESENTEE A MONACO PAR SA SUCCURSALE

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention n° 108 du Conseil de l'Europe 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, modifiée, relative à la protection des informations nominatives ;

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

Vu la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance d'application ;

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 ;

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, 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 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

Vu la Recommandation du Conseil de l'Europe n° R(89)2 du 19 janvier 1989 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;

Vu la délibération n° 2012-119 de la Commission de Contrôle des Informations Nominatives du 16 juillet 2012 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle* » utilisés à des fins de contrôle de l'activité des employés ;

Vu le traitement d'informations nominatives ayant pour finalité « *Finalité ordinaire d'envoi et de réception de correspondances électroniques* », dénommé « *Messagerie Professionnelle* », mis en œuvre par la Banca Popolare di Sondrio, le 2 septembre 2014 ;

Vu la délibération n° 2014-131 du 17 septembre 2014 portant décision de fixer des délais plus brefs que ceux prévus à la déclaration relative à la mise en œuvre du traitement ayant pour finalité « *Finalité ordinaire d'envoi et de réception de correspondances électroniques* » ;

Vu la demande d'autorisation déposée par la Banca Popolare di Sondrio (Suisse) S.A. (BPS Suisse), représentée à Monaco par sa succursale, le 8 septembre 2015, relative à la modification du traitement automatisé susvisé ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 6 novembre 2015, conformément à l'article 11-1 de la Loi n° 1.165, susmentionnée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 18 novembre 2015 portant examen du traitement automatisé susvisé ;

La Commission de Contrôle des Informations Nominatives,

Préambule

La Banca Popolare di Sondrio (Suisse) S.A. (BPS Suisse) est une société de droit suisse. Conformément aux dispositions de l'article 24 de la Loi n° 1.165, modifiée, elle est représentée en Principauté par sa succursale ayant pour activité « *la réalisation de toutes opérations de banque ou connexe telles que définies par la loi bancaire applicable* ».

Dans le cadre de l'exercice de leurs fonctions, les collaborateurs de la banque disposent d'une messagerie professionnelle. Aussi, la banque souhaite mettre en œuvre un système de supervision et de contrôle la messagerie électronique professionnelle.

A ce titre, en application de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, relatif à la mise en œuvre de traitements automatisés d'informations nominatives « *à des fins de surveillance* » ou « *portant sur des soupçons d'activités illicites, des infractions* », la Banca Popolare di Sondrio soumet la présente demande d'autorisation concernant le traitement ayant pour finalité « *Gestion et supervision de la messagerie professionnelle* ».

I. Sur la finalité et les fonctionnalités du traitement

La finalité du traitement est : « *Gestion et supervision de la messagerie professionnelle* ».

Le représentant du responsable de traitement indique que les personnes concernées sont « *tous les collaborateurs de la BPS (Suisse) ainsi que tout émetteur ou destinataire des emails* ».

Enfin, les fonctionnalités du traitement sont les suivantes :

« *Correspondre en interne avec l'ensemble des collaborateurs de la succursale et du groupe Banca Popolare di Sondrio (Suisse), ainsi qu'avec l'extérieur dans le cadre professionnel (fournisseurs, avocats, notaires, clients…).*

Il est à noter que l'utilisation de la messagerie professionnelle à des fins privées est autorisée.

Fonctionnalités :

- *répondre à une obligation légale ;*
- *garantir le respect d'un intérêt légitime du responsable du traitement et de son représentant ;*
- *permettre la constitution de preuve en cas de violation de ces intérêts ou en cas d'infractions civiles ou pénales ;*
- *échange de messages électroniques en interne ou avec l'extérieur ;*
- *historisation des messages électroniques entrants et sortants ;*
- *gestion des contacts de la messagerie électronique ;*
- *gestion des dossiers de la messagerie et des messages archivés ;*
- *établissement et lecture de fichiers journaux ;*
- *gestion des habilitations d'accès à la messagerie ;*
- *supervision messagerie professionnelle* ».

A la lecture de ce qui précède, la Commission précise que le traitement dont s'agit a notamment pour fonctionnalité de répondre aux obligations légales de vigilance et de traçabilité des opérations financières imposées notamment par la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, et 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.

Au vu de ces éléments, la Commission constate que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165, modifiée.

II. <u>Sur la licéité du traitement</u>

Conformément à l'article 11-1 de la Loi n° 1.165, modifiée, les traitements « *mis en œuvre à des fins de surveillance* » ou « *portant sur des soupçons d'activités illicites, des infractions* », doivent pour être licites être « *nécessaires à la poursuite d'un objectif légitime essentiel et [respecter] les droits et libertés mentionnés à l'article premier des personnes concernées (…)* ».

Dans sa délibération n° 2012-119 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle* » utilisés à des fins de contrôle de l'activité des employés, la Commission rappelle que conformément au principe de proportionnalité, le responsable de traitement est tenu de mettre en place une procédure de contrôle graduée, adaptée aux divers niveaux de risques auxquels il est confronté.

A cet égard, le représentant du responsable de traitement a annexé à la présente demande d'autorisation une circulaire interne relative à « *l'utilisation du courrier électronique et d'internet* ».

Relativement aux aspects particuliers de la surveillance des courriels, la Commission relève qu'un contrôle gradué en quatre phases est opéré au titre de l'analyse globale :

« *Phase 1 : le contrôle non nominatif global des fichiers journaux de la messagerie (ex. nombre de messages envoyés, format des pièces jointes, volumes, etc.) ;*

Phase 2 : le contrôle des fichiers journaux des messageries d'un ou plusieurs employés déterminés ;

Phase 3 : le contrôle du contenu des communications électroniques (archivées ou non) d'un ou plusieurs employés déterminés ou déterminables sélectionnés aléatoirement (échantillonnage) ou par filtrage automatique ;

Phase 4 : le contrôle du contenu des communications électroniques (archivées ou non) d'un ou plusieurs employés déterminés ».

Par ailleurs, elle observe que ladite circulaire définit une procédure précise quant au recours aux différentes phases d'analyse.

A cet égard, les analyses nominatives sont effectuées par le service des ressources humaines en collaboration avec le service informatique qui a la possibilité d'accéder « *en cas d'abus (…) aux informations contenues dans les archives e-mail sans aucune restriction sauf si le message est identifié comme privé (…) et le résultat de l'enquête [est] communiqué au niveau décisionnel approprié pour, le cas échéant, décider d'une sanction* ».

Sur ce point, la Commission constate qu'au sein dudit document un encart est destiné à appeler l'attention des utilisateurs : « *Veuillez spécifier dans le ligne « objet » lorsque le mail que vous désirez envoyer est privé en écrivant « Privé » ou « Personnel »* ».

Le représentant du responsable de traitement indique en outre que « *la Banque ne pourra alors pas accéder aux dits messages sauf sur autorisation du juge* ».

La Commission en prend donc acte.

Enfin, dans le but de limiter l'atteinte portée à la vie privée des employés, tout en permettant d'assurer la continuité des activités, elle demande, d'une part, que soient définies les procédures d'habilitation d'accès à la messagerie professionnelle en cas d'absence temporaire ou définitive d'un salarié de la banque, et d'autre part, que soit également assurée une traçabilité des consultations des données archivées.

A la condition de ce qui précède, la Commission considère que le traitement est licite, conformément aux dispositions légales.

III. Sur la justification du traitement

Le traitement est justifié par le respect d'une obligation légale à laquelle est soumis le responsable de traitement.

A cet égard, le représentant du responsable de traitement vise notamment les dispositions de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, de la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment, le financement du terrorisme et la corruption, et de la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou d'administration d'instruments financiers, toutes visées au V de la délibération n° 2012-119 du 16 juillet 2012 portant recommandation sur les traitement automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle* » utilisés à des fins de contrôle de l'activité des employés.

Ainsi, au vu de l'ensemble de ces éléments, la Commission considère que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165, modifiée.

IV. Sur les informations traitées

Les informations objets du traitement sont les suivantes :

- identité : nom, prénom, identifiant ;
- messages : contenu, objet, dossier de classement et archivage ;
- gestion des contacts : nom, prénom, sigle ;
- informations temporelles : date et heure ;
- données d'identification électronique : adresse de messagerie électronique ;
- logs d'accès : logs de connexion des personnels habilités ;
- fichiers journaux : nombres de messages entrants et sortants ;
- habilitations : identité des personnes habilitées à avoir accès.

En écho à ses remarques quant aux personnes concernées, la Commission estime que les informations relevant des catégories « *identité* » et « *messages* » sont issues des personnes concernées. Par ailleurs, le représentant du responsable de traitement indique que celles relatives à la « *gestion des contacts* » ont pour origine le salarié et le service informatique pour le sigle. Les « *informations temporelles* » sont enregistrées par le système Outlook. Enfin, les autres informations proviennent du Service informatique.

La Commission considère que ces informations 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, modifiée.

V. Sur les droits des personnes concernées

- ***Sur l'information des personnes concernées***

L'information préalable des personnes concernées est effectuée au moyen d'une procédure accessible en intranet. Une circulaire relative à « *l'utilisation du courrier électronique et d'internet* » a été annexée à la présente demande d'autorisation.

A cet égard, la Commission rappelle que conformément à l'article 14 de la Loi n° 1.165, modifiée, les personnes concernées doivent être informées de :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'identité des destinataires ou des catégories de destinataires des informations ;
- l'existence d'un droit d'accès et de rectification des informations les concernant.

Dans le cadre de sa délibération n° 2012-119, elle indique en outre qu'en cas de contrôle de la messagerie professionnelle, « *une telle obligation d'information relève d'un souci de transparence envers les employés, ainsi que de loyauté dans la relation de travail* ».

A cet égard, la circulaire susvisée prévoit que « *tous les collaborateurs de la Banque ont accès à tous les e-mails entrés ou sortis pendant toute la durée de conservation. Le Directeur est l'interlocuteur habilité à recevoir les demandes de droit d'accès. La personne exerçant son droit d'accès [doit] recevoir une réponse au plus tard 30 jours du jour de réception de sa demande* ».

Aussi, la Commission relève, d'une part, que le document d'information précité n'est pas conforme aux dispositions de l'article 14 de la Loi n° 1.165, précité, en ce qu'il ne mentionne pas la finalité exacte du traitement dont s'agit et les catégories de destinataires,

et d'autre part, que ladite circulaire à usage interne n'informe que le personnel de la banque alors même que les personnes concernées sont « *tous les collaborateurs de la BPS (Suisse) ainsi que tout émetteur ou destinataire des emails* ».

Elle demande donc que l'information préalable des personnes concernées soit complétée et portée à la connaissance de l'ensemble des personnes concernées, conformément à l'article 14 de la Loi n° 1.165, modifiée.

A cet effet, elle suggère qu'un avertissement (ou « *disclaimer* ») comportant ces mentions soit intégré en bas de chaque courriel, de sorte à informer les clients et des tiers expéditeurs ou destinataires des messages de leurs droits et de prévoir à ce titre les modalités de l'exercice de ces derniers.

- ***Sur l'exercice des droits d'accès, de rectification et d'opposition***

Les droits d'accès et de suppression s'exercent par courrier électronique auprès du Directeur de la succursale de Monaco. Le délai de réponse est de 30 jours.

Par ailleurs, la Commission observe que les messages archivés peuvent faire l'objet d'un contrôle ultérieur.

A cet égard, elle demande qu'un droit de suppression effectif soit instauré pour les collaborateurs à l'égard des messages dits « *privés* ».

Enfin, la Commission demande que l'ensemble des personnes concernées soient valablement informées des modalités d'exercice de leurs droits, conformément aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165, modifiée.

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

- ***Sur les destinataires***

Le représentant du responsable de traitement indique que les informations exploitées dans le cadre du traitement sont susceptibles d'être communiquées aux Services Informatique et Sécurité du siège de BPS (Suisse) à Lugano et à la Direction de la Sûreté Publique.

Aussi, la Commission estime qu'une communication à la Direction de la Sûreté Publique peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, elle rappelle qu'en cas de transmission, les Services de Police ne pourront avoir accès aux informations objets du traitement que dans le strict cadre de leurs missions légalement conférées.

Par ailleurs, elle considère que le SICCFIN peut être rendu destinataire des informations dans le cadre des dispositions de 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.

Ainsi, la Commission considère que ces communications d'information sont justifiées.

- ***Sur les personnes ayant accès au traitement***

Le représentant du responsable de traitement indique que les personnes habilitées à avoir accès aux informations en inscription, modification, mise à jour et consultation sont :

- les salariés du Service Informatique de la Banque BPS (Suisse) à Lugano ;
- les salariés du Service des Ressources Humaines de BPS (Suisse) succursale de Monaco ;
- le Directeur, l'Audit Interne (nommé également « Contrôle Interne »), et le Responsable du Service Juridique (nommé également « Legal & Compliance »).

Par ailleurs, la Commission estime que les expéditeurs et destinataires des courriels qui respectivement les reçoivent ou les envoient disposent également d'un accès aux informations.

Aussi, la Commission rappelle qu'en application de l'article 17-1 de la Loi n° 1.165, modifiée, une liste nominative des personnes ayant accès au traitement doit être tenue à jour, et doit pouvoir lui être communiquée à première réquisition.

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

VII. Sur les rapprochements et interconnexions avec d'autres traitements

Le représentant du responsable de traitement indique que le traitement dont s'agit ne fait l'objet d'aucun rapprochement ni aucune interconnexion.

A l'examen du dossier, la Commission relève qu'il fait l'objet d'une interconnexion avec un traitement systémique ayant pour finalité la gestion des accès et des habilitations (IAP administrator, Active Directory), non légalement mis en œuvre à ce jour.

En conséquence, elle demande que le traitement ayant pour finalité la gestion des accès et des habilitations soit légalement mis en œuvre dans les plus brefs délais.

VIII. 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'observations particulières.

La Commission relève cependant que l'architecture technique repose sur des équipements de raccordements (switchs) de serveurs et périphériques qui doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés.

La Commission rappelle néanmoins que, conformément à l'article 17 de la Loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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.

IX. Sur la durée de conservation

Le représentant du responsable de traitement indique que les informations nominatives collectées sont conservées pour une durée de 10 ans à l'exception des informations d'identité des salariés qui sont conservées « *pendant la durée du contrat du salarié avec la banque* ».

Par ailleurs, la Commission rappelle que dans le cadre de l'ouverture d'une procédure judiciaire, toute information nécessaire, notamment à des fins probatoires, pourra être conservée jusqu'au terme de la procédure.

Aussi, elle considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- conformément à l'article 17-1 de la Loi n° 1.165, modifiée, la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et doit pouvoir être communiquée à la Commission à première réquisition ;

- les équipements de raccordements de serveurs et périphériques doivent être protégés par un login et un mot de passe réputé fort et les ports non utilisés doivent être désactivés.

Demande :

- que soient définies les procédures d'habilitation d'accès à la messagerie professionnelle en cas d'absence temporaire ou définitive d'un salarié de la banque ;

- que soit assurée une traçabilité des consultations des données archivées ;

- que l'information préalable des personnes concernées soit complétée et portée à la connaissance de l'ensemble des personnes concernées ;

- qu'un droit de suppression effectif soit instauré pour les collaborateurs à l'égard des messages dits « *privés* » ;

- que l'ensemble des personnes concernées soient valablement informées des modalités d'exercice de leurs droits ;

- que l'interconnexion avec le traitement ayant pour finalité la gestion des accès et des habilitations soit interrompue jusqu'à ce qu'il soit légalement mis en œuvre.

A la condition de la prise en compte des éléments qui précèdent,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre, par LA BANCA POPOLARE DI SONDRIO (SUISSE) S.A. (BPS SUISSE), REPRESENTEE A MONACO PAR SA SUCCURSALE, du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie professionnelle* ».**

Le Président

Guy MAGNAN