Délibération n° 2017-165 du 20 septembre 2017

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

« *Supervision des activités sur la base de données documentaire, dénommé Application « Arel »* »

présenté par BANCA POPOLARE DI SONDRIO (SUISSE) SA

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne 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° 1.338 du 7 septembre 2007 sur les activités financières ;

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

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° 1.284 du 10 septembre 2007 portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, susvisée ;

Vu l'Arrêté français du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution ;

Vu la Recommandation CM/Rec(2015)5 du Conseil de l'Europe du 1er avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi ;

Vu la demande d'autorisation déposée le 30 mai 2017 par Banca Popolare di Sondrio (Suisse) SA, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Supervision des activités sur la base de données documentaire* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 27 juillet 2017, 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 septembre 2017.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Banca Popolare Di Sondrio (BPS) est une société suisse qui est établie à Monaco par sa succursale enregistrée au RCI sous le numéro 03S04108, ayant entre autres pour objet « *la réalisation de toutes opérations de banque ou connexe telles que définies par la loi bancaire applicable* ».

Dans le cadre de son organisation interne, et afin d'assurer la sécurité informatique de son réseau et la confidentialité des informations qu'il contient, la banque souhaite mettre en œuvre un traitement ayant pour finalité « *Supervision des activités sur la base de données documentaire » dénommé « Application « Arel » »*.

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, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement soumis a pour finalité « *Supervision des activités sur la base de données documentaire*, *dénommé Application « Arel » ».*

Il concerne les salariés de la succursale monégasque de BPS.

Il a pour fonctionnalité de journaliser l'activité des salariés de la banque sur la base documentaire en vue de détecter d'éventuels manquements aux obligations du secret professionnel.

La Commission relève également à l'analyse du dossier qu'il permet l'envoi par email interne au personnel du service « *Contrôle des risques* » sis à Lugano en Suisse, à des fins de vérification et de contrôle :

- Quotidiennement les logs contenant les actions d'impression effectuées sur le présent traitement ;
- Mensuellement les logs d'impression et de consultation réalisés sur les documents présents sur cette base de données documentaire.

La Commission relève que le contrôle est effectué manuellement, et non de manière automatisée, aux fins de déceler un éventuel comportement à risque, et que le collaborateur concerné est informé et amené à s'expliquer en cas de soupçon. Elle relève donc que l'article 14-1 de la Loi n° 1.165 ne s'applique pas au présent traitement.

Par ailleurs, elle constate que les salariés ne font pas l'objet d'un contrôle permanent et inopportun. En effet, seule leur activité sur la base documentaire est surveillée. Toute activité autre au sein du système d'information de la banque est loguée sans surveillance, en conformité avec la déclaration relative à la « *Gestion administrative des salariés* », valablement mise en œuvre par le responsable de traitement.

La Commission considère que la finalité du traitement est explicite et légitime, conformément à 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 justifié par le respect d'une obligation légale, par l'exécution d'un contrat ou de mesures pré-contractuelles avec la personne concernée et par la réalisation d'un intérêt légitime, sans que soient méconnus ni l'intérêt ni les libertés et droits fondamentaux des personnes concernées.

A cet égard, il indique que la :

- « *Loi n° 1.338 sur les activités financières et notamment son article 33 qui dispose que « toute personne physique qui, à un titre quelconque, participe à l'administration, à la direction ou à la gestion d'une société agréée ou qui est employée par celle-ci est tenue au secret professionnel dans les conditions et sous les peines prévues à l'article 308 du Code Pénal […] » ;*
- *Loi n° 1.314 relative à l'exercice d'une activité de conservation ou d'administration d'instruments financiers et notamment son article 3 qui dispose que « le teneur de compte-conservateur doit disposer des moyens et procédures nécessaires à l'exercice de son activité, notamment, en ce qui concerne les ressources humaines, les moyens informatiques, la comptabilité, les dispositifs de protection de la clientèle et les contrôles internes, tels que définis par arrêtés ministériels » ».*

Par ailleurs, la Commission relève qu'il résulte de l'article 11 du Titre II - Le système de contrôle des opérations et des procédures internes - de l'Arrêté français du 3 novembre 2014, susvisé, que le responsable de traitement a l'obligation « *de vérifier les conditions d'évaluation, d'enregistrement, de conservation et de disponibilité de [l'information comptable et financière] notamment en garantissant l'existence de la piste d'audit au sens de l'article 85* » et de « *vérifier la qualité des systèmes d'information et de communication* », et que les articles 6, 7 et 11 de l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 contiennent des dispositions comparables.

En outre en l'absence de précision quant aux libertés et droits fondamentaux des personnes concernées et notamment des salariés de la banque, la Commission demande que le responsable de traitement s'assure que les personnes concernées bénéficient d'une information préalable claire quant à l'existence du traitement dont s'agit, aux droits dont elles disposent relativement au traitement et à leurs modalités d'exercice.

Aussi, elle considère que ce traitement est licite et justifié, au sens des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

Toutefois, la Commission relève que l'exécution d'un contrat ou de mesures pré-contractuelles avec la personne concernée n'est pas un critère valable permettant de justifier de la licéité du présent traitement.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- journaux : horodatage (date + heure) de l'évènement ; nom d'utilisateur source de l'évènement ; matricule de l'utilisateur lié à l'évènement ; évènement journalisé : impression de documents, consultation de documents, création de documents, changement d'un attribut du document ; dossier de classement du document concerné par l'évènement ; numéro de relation client concerné par l'évènement ; description du document lié à l'évènement ; référence unique du document.

  Les informations proviennent du logiciel.

La Commission considère 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 personnes concernées est assurée au moyen d'une procédure interne accessible en Intranet.

Toutefois, le document susvisé n'étant pas joint à la présente demande, la Commission n'est pas en mesure de s'assurer que l'information préalable des salariés est conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Aussi elle rappelle que l'information de l'ensemble des personnes concernées doit être assurée conformément à 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 :***

Les droits d'accès, de modification, de mise à jour et de suppression s'exercent par voie postale ou sur place auprès du Directeur de BPS (Suisse) – succursale de Monaco.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit intervenir dans le mois suivant la réception de la demande.

Elle constate 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 personnes ayant accès au traitement et les communications d'informations

➢ ***Sur les accès au traitement***

Le responsable de traitement indique que les personnes habilitées à avoir accès au traitement sont :

- la Direction de la succursale à Monaco : en consultation ;
- le personnel du Service Contrôle Interne de la succursale à Monaco : en consultation ;
- le personnel du Service Contrôle des Risques de BPS Suisse (Maison Mère) : en consultation ;
- le personnel du Service Informatique de BPS Suisse (Maison Mère) dans la limite de ses missions de maintenance : en inscription, mise à jour, modification, consultation.

La Commission souligne qu'en cas de recours à des prestataires, leurs accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, conformément à l'article 17 de la Loi n° 1.165. De plus ils sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement.

Elle rappelle 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 doit être tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

Elle considère que ces accès sont justifiés.

- ***Sur les communications d'informations***

Il est indiqué que des informations peuvent être communiquées à la maison mère, sise en Suisse.

La Commission relève par ailleurs qu'elles peuvent être communiquées à la Direction de la Sûreté Publique à Monaco, aux Tribunaux et Cours à Monaco et à l'ACPR en France.

La Commission considère que ces communications d'informations sont justifiées.

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

Le responsable de traitement indique que le présent traitement est interconnecté avec les traitements ayant pour finalités respectives « *Gestion des habilitations* » et « *Gestion et supervision de la messagerie professionnelle* », légalement mis en œuvre.

La première interconnexion concerne l'habilitation des personnels sur le système d'information de la succursale, qui détermine en amont les droits des personnels sur la base documentaire. Seule l'activité sur cette base documentaire fait l'objet d'une surveillance.

La seconde interconnexion permet l'envoi automatique des fichiers journaux au service contrôle des risques, tel que décrit au point I de la présente délibération.

La Commission constate que ces interconnexions sont conformes aux exigences légales.

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.

Cependant les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

La Commission rappelle enfin 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 la durée de conservation

Le responsable de traitement indique que les informations nominatives collectées sont conservées 3 ans.

La Commission considère que cette durée de conservation est disproportionnée au regard de la finalité du traitement.

Aussi, elle fixe la durée de conservation à 1 an maximum à compter de leur collecte, s'agissant de ces fichiers journaux.

Après en avoir délibéré, la Commission :

Rappelle que :

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

- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et 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 les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

Demande que le responsable de traitement s'assure que les personnes concernées bénéficient d'une information préalable claire quant à l'existence du traitement dont s'agit, aux droits dont elles disposent relativement au traitement et à leurs modalités d'exercice.

Fixe la durée de conservation des informations à 1 an maximum à compter de leur collecte, s'agissant des « *fichiers journaux* » ;

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 Banca Popolare di Sondrio (Suisse) SA, du traitement automatisé d'informations nominatives ayant pour finalité « *Supervision des activités sur la base de données documentaire, dénommé « Application Arel »* ».**

Le Président

Guy MAGNAN