Délibération n° 2023-020 du 15 février 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 et supervision des droits et habilitations* »

présenté par Bank Julius Baer & Co. Ltd,

représenté en Principauté par Bank Julius Baer (Monaco) S.A.M.

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 Bank Julius Baer & Co. Ltd, représentée en Principauté par Bank Julius Baer (Monaco) S.A.M., le 15 novembre 2022 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et supervision des droits et habilitations* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 13 janvier 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 15 février 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Bank Julius Baer & Co. Ltd est une société suisse représentée en Principauté par Bank Julius Baer (Monaco) S.A.M., une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 96S03173, ayant entre autres pour objet *« en Principauté de Monaco et à l'étranger, pour son compte ou le compte de tiers, directement ou en participation : 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 (S.I.), 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 et supervision des droits et habilitations ».*

Les personnes concernées sont les salariés et les prestataires externes.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

Dans le cadre de la gestion des habilitations *:*

- octroyer / délivrer aux utilisateurs du S.I. 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 des comptes systèmes dans le cadre de changement 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 les Lois n° 1.314 du 29 juin 2006, n° 1.338 du 7 septembre 2007 et n° 1.362 du 3 août 2009 ainsi que par l'Arrêté Ministériel n° 2012-199 du 5 avril 2012.

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 de ses employés ;*
- *La sécurité et le bon fonctionnement technique du réseau 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* ».

Le responsable de traitement précise en outre que le présent traitement « *permet d'assurer la confidentialité des données, notamment des données de client* ».

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 du salarié ou du prestataire externe, nom du manager ;
- adresses et coordonnées : adresse email professionnelle, numéros de téléphone fixe et mobile professionnels ;

- formation, diplômes, vie professionnelle : poste occupé, grade, droits conférés ;
- données d'identification électronique : identifiants de la personne habilitée ;
- informations temporelles : logs d'administration, datation de la création des accès, logs relatifs aux actions réalisées sur les serveurs hébergeant le traitement, logs temporels de connexion et déconnexion aux serveurs.

Le responsable de traitement indique que les informations relatives à l'identité, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle ainsi que les données d'identification électronique ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* ».

La Commission considère toutefois que pour les prestataires externes ces informations peuvent également avoir pour origine le contrat de prestation de service.

Le responsable de traitement indique par ailleurs que les informations temporelles ont pour origine le service IT.

La Commission considère toutefois que celles-ci ont pour origine le système du présent traitement.

Elle constate 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 clause incluse dans le contrat de travail et d'une procédure interne accessible en Intranet.

A cet égard, la Commission rappelle que l'information préalable doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993.

Elle rappelle également que cette information préalable doit s'effectuer auprès de l'ensemble des personnes concernées, à savoir y compris les prestataires externes.

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

Le droit d'accès s'exerce par voie postale, par courrier électronique et sur place auprès du Directeur juridique et Data Protection Officer.

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

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, elle considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous cette condition, la Commission estime 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 policières ou judiciaires légalement habilitées.

La Commission 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 salariés Julius Baer des services IT (Suisse, Luxembourg, Monaco) : tous droits ;
- les prestataires externes évoluant sur l'environnement IT du groupe Julius Baer (Suisse, Luxembourg, Monaco) : consultation et maintenance ;
- les salariés Julius Baer : consultation des droits qui leurs sont conférés.

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

En ce qui concerne les prestataires, la Commission 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.

Elle rappelle par ailleurs 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.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement est interconnecté avec le traitement ayant pour finalité « *Gestion administrative des salariés* », légalement mis en œuvre.

Il indique également qu'il fait l'objet d'interconnexions avec tous les traitements déjà mis en place ou à venir faisant appel au système d'habilitation dont s'agit.

La Commission en prend acte et considère 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 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.

VIII. Sur les durées de conservation

Le responsable de traitement indique que les informations relatives à l'identité, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle ainsi que les données d'identification électronique sont conservées 3 mois suivant le départ du salarié et que les informations temporelles sont conservées 1 an.

A cet égard, conformément à sa délibération n° 2017-206 du 20 décembre 2017, la Commission fixe toutefois la durée de conservation des données d'identification électronique à la durée d'utilisation du S.I. par la personne concernée.

Sous cette réserve, elle considère que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle que :

- l'information préalable doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993 ;
-
- cette information préalable doit s'effectuer auprès de l'ensemble des personnes concernées, à savoir y compris les prestataires externes ;

- la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;

- 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, doit être tenue à jour et 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.

Fixe la durée de conservation des données d'identification électronique à la durée d'utilisation du S.I. par la personne concernée.

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 Bank Julius Baer & Co. Ltd, représentée en Principauté par Bank Julius Baer (Monaco) S.A.M. , du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision des droits et habilitations* ».**

Le Président

Guy MAGNAN