Délibération n° 2024-093 du 17 avril 2024

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

« *Mise à disposition et supervision d'un système de messagerie instantanée -E-services* »

dénommé « *BJB Chat* »

présenté 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 n° Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive et la corruption ;

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

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 ;

Vu l'Ordonnance n° 3.559 du 5 décembre 2011 rendant exécutoire l'Accord monétaire entre l'Union européenne et la Principauté de Monaco ;

Vu la délibération n° 2023-100 du 19 juillet 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 de la messagerie*

électronique professionnelle à des fins de surveillance et de contrôle » présenté par Bank Julius Baer (Monaco) S.A.M.

Vu la demande d'autorisation déposée par Bank Julius Baer (Monaco) S.A.M., le 10 janvier 2024, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Mise à disposition d'un système de messagerie instantanée – E -Services* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 7 mars 2024, 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 17 avril 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Bank Julius Baer (Monaco) S.A.M. est une société anonyme monégasque, immatriculée au répertoire du Commerce et de l'Industrie sous le numéro 96S03173, qui a notamment 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 ; Et généralement, toutes les opérations sans exception, civiles, financières, commerciales, industrielles, mobilières ou immobilières pouvant se rapporter directement à l'objet social ci-dessus ou susceptibles d'en favoriser le développement* ».

Cette société indique que « *Le traitement a pour objectif de donner la possibilité à un client ayant souscrit une offre d'E-service de communiquer avec son gestionnaire par le biais d'un canal sécurisé utilisant l'application WhatsApp (côté client) et une interface web dédiée et sécurisée (coté gestionnaire*) ».

Ledit traitement étant mis en œuvre à des fins de surveillance, le responsable de traitement sollicite, conformément aux dispositions de l'article 11-1 de la Loi n° 1.165, l'autorisation de la Commission.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Mise à disposition d'un système de messagerie instantanée-E-services* ».

Le responsable de traitement indique que sont concernés par le présent traitement ses clients et ses salariés.

Entant précisé que « *Les communications qui transitent sur ce canal sont exclusivement des informations « Business related »* », les fonctionnalités sont :

- instructions du client pour le transfert de fonds et de titres ;
- instructions du client pour les opérations sur titres ;
- communication de modifications relatives à la personne : détails de contact, adresse, numéro de téléphone, toute information relative à la gestion du compte (ces informations sont communiquées par le client dans le fil de discussion) ;
- contenu du message uniquement ;

- contrôle et analyse des données transmises par le biais du canal afin de prévenir et détecter les fuites de données (DLP) ;
- constitution de preuve en cas de litige.

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.

Aussi, en l'espèce, elle considère que la finalité du traitement doit être plus explicite et indiquer qu'il existe une surveillance des fuites de données.

En conséquence, la Commission modifie la finalité comme suit : « *Mise à disposition et supervision d'un système de messagerie instantanée -E-services* ».

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 à laquelle il est soumis et l'exécution d'un contrat avec la personne concernée.

Il précise que l'utilisation de ce canal résulte du contrat de E-service, facultatif, conclu entre la Banque et son client.

La Commission relève en outre que la conservation des informations objet du traitement est rendue obligatoire en application des dispositions de la Loi n° 1.338 sur les activités financières, de son Ordonnance d'application, ainsi que de l'article 23 de la Loi n° 1.362 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive et la corruption.

Enfin, le responsable de traitement indique que la mise en œuvre du DLP lui permet de répondre à ses obligations de respect du secret professionnel et du secret bancaire, et de répondre aux exigences de l'Arrêté français du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, et notamment à son article 270-3 qui prévoit la mise en œuvre d'une procédure de sécurité assurant la protection de la confidentialité et de l'intégrité des données.

Aussi, la Commission considère que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165, modifiée.

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- identité : nom, prénom des clients et gestionnaires ;
- adresses et coordonnées : numéro de téléphone mobile et/ou adresse email ;
- informations temporelles : identifiants de connexion et logs de connexion des personnels habilités à avoir accès au traitement, date et heure d'envoi/réception du message ;
- données relatives au traitement : contenu de la discussion ;
- alertes Data Loss Prevention : réception et traitement des alertes sur l'outil « *Data Loss Prevention* ».

L'origine des informations n'appelle pas d'observations.

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'un document spécifique, d'une mention particulière intégrée dans un document remis à l'intéressé, d'un courrier adressé à l'intéressé ainsi que par le biais d'une rubrique propre à la protection des données accessible en ligne.

Outre les Conditions Générales (General Business Conditions) et la « *Privacy Notice of Bank Julius Baër (Monaco) S.A.M. on the processing of personnal data in accordance with the EU general data protection regulation (GDPR)* », un document spécifique est remis au client pour utiliser WhatsApp dans ses relations avec la Banque. Ces documents, en langue anglaise, n'informent pas le client de manière conforme aux dispositions de l'article 14 de la Loi n° 1.165 relativement au présent traitement.

Il résulte toutefois des informations communiquées par la Banque qu'avant de pouvoir utiliser ce canal, un client qui utilisait au préalable le E-service doit nécessairement lire et accepter les conditions d'utilisation qui lui sont dédiées. La Commission estime ainsi qu'il s'agirait de l'étape la plus adaptée pour procéder à l'information des personnes concernées.

Elle demande donc que ce document, non communiqué, contienne une information conforme aux dispositions de l'article 14 de la Loi n° 1.165, disponible également en langue française.

La Commission rappelle enfin que WhatsApp est une solution du groupe Meta qui, bien que chiffrée de bout en bout et soumise au Digital Service Act, peut poser des questions de confidentialité et de sécurité.

Elle relève toutefois qu'il s'agit d'une option activée par le client et que ce dernier est informé par l'établissement bancaire, au sein du « *document spécifique* » susvisé, des risques liés à son utilisation (confidentialité, communications de données entre entités du groupe Meta et potentiellement vers des pays non adéquat). La Commission recommande que cette information soit incluse dans les conditions d'utilisation, en langue française si nécessaire, et qu'elle prenne en compte le droit monégasque, et non uniquement Suisse.

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

Le responsable de traitement indique que le droit d'accès s'exerce auprès du Directeur Juridique et Data Protection Officer par voie postale, sur place ou par courrier électronique.

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 en cas de doute 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 ces conditions, 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 personnes ayant accès au traitement et les communications d'informations

- ***Sur les accès au traitement***

Les personnes ayant accès au traitement sont :

- la personne concernée, en inscription, consultation, modification ;
- le gestionnaire ou l'assistant, en consultation et modification ;
- le Service informatique, à des fins de maintenance sans accès à l'interface du client, sans accès au contenu des messages échangés ;
- le Service IT impliqué dans la gestion DLP et l'équipe de monitoring DLP : modification, consultation, maintenance aux alertes DLP (uniquement dans le cadre de l'alerte remontée dans le système DLP et non au contenu du message).

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

La Commission rappelle que conformément à l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993, le responsable de traitement est tenu de « *déterminer nominativement la liste des personnes qui ont seul accès, pour les stricts besoins de l'accomplissement de leurs missions, aux locaux et aux installations utilisées pour les traitements, de même qu'aux informations traitées* ». Elle rappelle de plus que cette liste doit être tenue à jour et précise qu'elle doit lui être communiquée à première réquisition.

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

Le responsable de traitement indique que les informations collectées peuvent être communiquées aux Autorités habilitées. La Commission en prend acte.

VI. Sur les rapprochements et les interconnexions

Le responsable de traitement indique que le présent traitement est interconnecté avec les traitements légalement mis en œuvre suivants :

- gestion administrative des salariés, afin d'utiliser le nom et le prénom du gestionnaire lors de la création de l'instance avec le client ;
- tenue des comptes de la clientèle et le traitement des informations s'y rattachant, afin d'y consigner les échanges relatifs à une opération, un mouvement, un ordre ;
- gestion et supervision de la messagerie électronique professionnelle à des fins de surveillance et de contrôle, afin de monitorer le DLP sur BJB Chat ;
- gestion du support et développement informatique, à des fins de maintenance réalisée par le Service IT ;
- mise à disposition de Services de Banque à distance (Services Internet et Internet mobile)

La Commission constate que ces interconnexions sont compatibles avec les finalités initiales des traitements mis en œuvre et sont donc 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.

Par ailleurs, elle rappelle que les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

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 sont conservées « *5 ans à compter de la création de la discussion* », étant précisé que chaque session ouverte par un client s'analyse en une conversation unique.

La Commission constate ainsi que la durée est conforme aux dispositions de la Loi n° 1.338 sur les activités financières et de son Ordonnance d'application, et à l'article 23 de la Loi n° 1.362 du 3 août 2009, modifiée.

Par ailleurs, il précise qu'en ce qui concerne les informations en lien avec les alertes Data Loss Prevention, ces dernières sont conservées 5 ans à réception de l'alerte.

Cette durée est conforme à l'autorisation délivrée par la Commission par délibération n° 2023-100 du 19 juillet 2023 relativement à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie électronique professionnelle à des fins de surveillance et de contrôle* ».

La Commission rappelle toutefois avoir demandé que les données relatives à un évènement ne mettant pas en lumière un incident (faux positifs par exemple) soient immédiatement supprimées après analyse.

Sous cette réserve, la Commission considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

- **Demande que** l'information des personnes concernées soit s'effectuée de manière conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993, de préférence au sein des conditions d'utilisation du dispositif, et que la mention d'information soit disponible en langue française.

Rappelle que :

- s'agissant des alertes générées, les données relatives à un évènement ne mettant pas en lumière un incident (faux positifs par exemple) doivent être immédiatement supprimées après analyse ;

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

- les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises ;

- une procédure relative au droit d'accès par voie électronique doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agisse effectivement de la personne concernée par les informations.

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 Bank Julius Baer (Monaco) S.A.M., du traitement automatisé d'informations nominatives ayant pour finalité « *Mise à disposition et supervision d'un système de messagerie instantanée -E-services* ».**

Le Président

Guy MAGNAN