بنك المغرب
BANK AL-MAGHRIB

Le Gouverneur الوالي

D N° 4/W/2022 **Rabat, le 19 Mai 2022**

Directive fixant les règles minimales en matière d'externalisation vers le cloud par les établissements de crédit

Le Wali de Bank Al-Maghrib ;

Vu la loi n°103-12 relative aux établissements de crédit et organismes assimilés promulguée par le dahir n° 1-14-193 du 1er rabii I 1436 (24 Décembre 2014) ;

Vu les dispositions de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;

Vu les dispositions de la loi 05-20 relative à la cybersécurité promulguée par le dahir n° 1-20-69 du 25 Juillet 2020 ;

Vu les dispositions de la circulaire n°4/W/2014 du 30 octobre 2014 relative au contrôle interne des établissements de crédit ;

Vu les dispositions de la directive n°3/W/2016 fixant les règles minimales à observer par les établissements de crédit pour réaliser les tests d'intrusion des systèmes d'information ;

Vu les dispositions de la Directive Nationale de la Sécurité des Systèmes d'Information ;

Vu la délibération N° D-110-2021 du 30/04/2021 de la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel portant avis sur le projet de directive fixant les règles minimales en matière d'externalisation vers le Cloud par les établissements de crédit.

Après avis du Comité des établissements de crédit émis en date du 16 mai 2022 ;

Fixe par la présente directive les règles minimales devant être observées par les établissements de crédit et organismes assimilés, désignés ci-après « établissement (s) », en matière d'externalisation vers le Cloud.

Article 1

Les dispositions de la présente directive constituent des normes minimales. Les établissements de crédit prennent toute mesure supplémentaire qui s'avèrerait nécessaire pour gérer les risques inhérents à l'externalisation vers le Cloud.

Ces normes s'appliquent sans préjudice des règles plus contraignantes prévues par les dispositions légales et réglementaires en vigueur.

Article 2

Pour les besoins de la présente directive, on entend par :

Cloud : Un modèle technologique qui permet un accès, à la demande, à un ensemble de ressources informatiques partagées et configurables (ex. réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement fournies et libérées par un minimum d'effort de gestion ou d'interaction de la part du fournisseur de services Cloud. Le Cloud Computing est généralement composé de plusieurs types de services (logiciels, plateformes, infrastructures... en tant que service) et modèles de déploiement (public, privé, hybride...).

Fournisseur de services Cloud (FSC) : Tiers qui met à disposition des services Cloud. Ce tiers peut être aussi une filiale ou une entreprise mère de l'établissement

Fonction : Tout ou une partie d'un Système d'information, processus, service ou activité de l'établissement.

Fonction significative : Fonction dont toute perturbation induirait un effet significatif sur la maitrise des risques de l'établissement et la continuité de ses activités.

Externalisation en chaine ou en cascade : Le cas où le FSC externalise certaines tâches spécialisées de sa chaîne de production à des tiers.

Indicateurs clés de performance (Key Performance Indicator – KPI) : toute évaluation calculable sur la base d'un ensemble de métriques reflétant la qualité d'un service de Cloud.

Engagement de service (Service Level Agreement – SLA) : les engagements spécifiant l'ensemble des objectifs et des niveaux de services à fournir par le FSC à l'établissement.

Stratégie de sortie : plan permettant à l'établissement de mettre un terme au contrat de prestation le liant à un FSC, tout en minimisant les impacts en découlant.

Clause de réversibilité : clause contractuelle permettant à un établissement ayant externalisé ses fonctions à un FSC de récupérer ses données à l'issue du contrat.

TITRE I : Cadre de gouvernance du recours au Cloud

Article 3

L'organe d'administration de l'établissement approuve la stratégie et la politique adoptées en matière d'externalisation vers le Cloud et veille au respect des dispositions de la présente directive et des lois et réglementations en la matière. Dans ce cadre, Il doit notamment :

a. S'assurer de la définition d'une stratégie et d'une politique d'externalisation vers le Cloud, cohérentes avec la stratégie informatique et la politique de sécurité des systèmes d'information de l'établissement ;

b. Surveiller les risques encourus par l'externalisation vers le Cloud ;

c. S'assurer de la mise en place de moyens humains, matériels et techniques nécessaires au suivi et au contrôle des fonctions externalisées vers le Cloud et à la mitigation des risques y afférents ;

d. Attribuer les rôles et responsabilités en matière de documentation, de gestion et de contrôle des dispositifs d'externalisation vers le Cloud.

Article 4

L'établissement met en place un dispositif formalisé et approuvé de gestion des risques au regard de l'usage du Cloud, conforme aux dispositions légales et réglementaires en vigueur.

Article 5

L'établissement met en place un dispositif formalisé et approuvé de gestion de ses données, en intégrant notamment :

a. La classification des données de l'établissement selon une approche basée sur les risques ;

b. Les localisations éligibles à l'hébergement des données selon leur classification ;

c. Les solutions Cloud applicables aux données selon leur classification ;

d. Les mesures de sécurité et restrictions applicables aux données selon leur classification ;

e. Les processus de récupération suite à une perte ou une violation de la sécurité des données.

Article 6

Le dispositif de contrôle des fonctions externalisées vers le Cloud doit faire partie intégrante du dispositif de vérification des opérations et procédures internes au sens de la circulaire du contrôle interne susvisée. L'établissement s'assure que :

a. La politique d'externalisation vers le Cloud est conforme aux lois et règlements applicables et effectivement mise en œuvre et cohérente avec son dispositif de gestion des risques ;

b. Les dispositifs de classification des données et de gestion des risques d'externalisation vers le Cloud sont formalisés et mis en œuvre ;

Les mesures de sécurité mises en place sont adaptées à la criticité des fonctions externalisées.

TITRE II : Prérequis avant toute externalisation vers le Cloud

Article 7

L'établissement examine l'opportunité de recours au Cloud au regard des risques potentiels encourus, en particulier, en matière de conformité aux dispositions légales et réglementaires qui lui sont applicables.

Article 8

Avant d'entreprendre toute externalisation des fonctions vers le Cloud, l'établissement conduit une analyse des risques lui permettant de déterminer ses fonctions significatives, de classer ses données et d'identifier les solutions Cloud et les mesures de sécurité adéquates. Dans le cadre de cette analyse, les principaux risques à considérer par l'établissement sont :

a. La perte de gouvernance sur le traitement ;

b. La dépendance technologique vis-à-vis du FSC ;

c. Le non-respect des exigences de l'établissement en matière de disponibilité, d'intégrité et de confidentialité des données hébergées suite à une défaillance du FSC ou à une mauvaise gestion de l'externalisation ;

d. L'exécution de réquisitions judiciaires sur la base de droit étranger sans concertation avec les autorités nationales ;

e. La défaillance au niveau de la chaîne de sous-traitance, dans le cas où le FSC lui-même fait appel à des tiers pour fournir le service dans le cadre d'une externalisation en chaine ;

f. Le non-respect des règles de conservation et de destruction des données de l'établissement, ou par leur conservation au-delà de la durée convenue ;

g. La gestion ineffective des droits d'accès induite par une insuffisance des moyens fournis par le FSC ;

h. La fin de fourniture du service du FSC ou l'acquisition de ce dernier par un tiers ;

i. La non-conformité réglementaire du FSC sur les transferts internationaux des données ;

j. La défaillance dans l'interconnexion et l'interfaçage entre le système d'information de l'établissement et celui du prestataire Cloud (non chiffrement, faiblesses de l'authentification, Incompatibilité de protocoles, failles sur les APIs, ...) ;

k. La défaillance dans la gestion des ressources mutualisées (Réseaux, Liens d'accès, Stockage, Serveurs, Sécurité, ...) ;

l. La défaillance du prestataire en matière de gestion des clés cryptographiques et de la flexibilité qu'il propose aux établissements de disposer de leurs propres clés en local ou en Cloud ;

m. La non communication (manque de transparence) à l'établissement des faiblesses techniques ou incidents de sécurité impactant directement ou indirectement les services Cloud.

Article 9

L'établissement s'assure que le FSC :

a. Est conforme au cadre légal et réglementaire régissant ses activités ;

b. Présente les garanties suffisantes notamment au plan de la gouvernance, de la réputation et du contrôle interne ;

c. Dispose de plans de continuité d'activité testés et en phase avec les exigences de l'établissement en matière de disponibilité, d'intégrité et de confidentialité ;

d. Met en œuvre un dispositif de gestion des risques et évalue périodiquement ces derniers ;

e. Dispose de certifications garantissant la qualité et la sécurité des services fournis ;

f. Démontre une solidité financière et des ressources suffisantes permettant de respecter ses engagements ;

g. Présente les références et l'expérience nécessaires auprès d'autres établissements comparables ;

h. Dispose de mesures de sécurité et de sûreté physique sur ses sites d'hébergement conformément aux normes et standards internationaux en la matière ;

i. Possède les capacités à identifier et à cloisonner les données de l'établissement à l'aide de contrôles physiques ou logiques ;

j. Dispose d'une capacité pour effectuer de manière efficace ses prestations de service ;

k. Communique à l'établissement les technologies et l'architectures mises en œuvre pour la réalisation des prestations demandées ;

l. Dispose d'une assurance cyber sécurité couvrant tout risque de violation des données.

L'établissement doit mener un processus de diligence raisonnable complet pour le choix du FSC comprenant des évaluations indépendantes en plus des attestations du prestataire de services et/ou des références des clients. La rigueur et la profondeur de la diligence raisonnable entreprise par l'établissement devraient être proportionnelles à l'évaluation des risques et tenir compte de la criticité et de la sensibilité des actifs concernés et du niveau de confiance que l'établissement accorde au prestataire pour maintenir des contrôles de sécurité efficaces.

Ce processus et ces conditions doivent être soumis aux organes de gouvernance et au comité d'audit ou des risques, selon le cas, au préalable.

Article 10

L'établissement s'assure, de manière continue, que :

- les politiques gouvernementales, les conditions politiques, sociales et économiques et les développements juridiques et réglementaires dans les pays d'hébergement de ses données ne présentent pas de risques pouvant impacter son recours au Cloud.
- les pays de localisation éligibles à l'hébergement des données doivent être appréciés en fonction des garanties apportées en matière de protection des données à caractère personnel notamment par le choix de pays assurant une protection suffisante de ces données.
- Ses exigences relatives à la localisation de ses données sont respectées, à travers notamment :

  a. L'engagement du FSC à lui communiquer la localisation de ses données hébergées dans le Cloud à tout moment ;

  b. L'assurance que les localisations d'hébergement des données proposées par le FSC n'empêchent pas l'établissement de respecter ses engagements ;

  c. La capacité de contrôler les accès à ses données hébergées dans différentes juridictions ;

  d. La maitrise des risques induits par le recours aux services Cloud dans d'autres juridictions ;

  e. La prise en compte des différences entre les juridictions en ce qui concerne la protection des données.

Article 11

L'établissement s'assure que le FSC maîtrise les risques encourus pour toute sous-traitance ou externalisation en chaîne. Il tient compte notamment du risque de réduction de la capacité à contrôler et surveiller les fonctions externalisées.

Article 12

Tout projet d'externalisation de l'établissement de ses fonctions significatives vers le cloud doit recueillir l'accord préalable de Bank Al-Maghrib.

Bank Al-Maghrib peut avoir accès, à tout moment, aux informations relatives aux fonctions externalisées. L'établissement prend les mesures nécessaires pour s'en assurer.

Article 13

L'établissement se dote d'un plan de continuité d'activité mis à jour, testé régulièrement qui tient compte des risques liées à l'externalisation vers le Cloud.

Article 14

L'établissement tient à jour une stratégie de sortie documentée et cohérente avec sa politique d'externalisation vers le Cloud et son plan de continuité d'activité. Cette stratégie doit être constituée des éléments suivants :

a. Les critères déclencheurs de sortie des contrats d'externalisation vers le cloud, tels que définis dans lesdits contrats, liant l'établissement au fournisseur de services Cloud, notamment :

   i. La résiliation des contrats d'externalisation vers le Cloud ;

   ii. La défaillance du fournisseur de services Cloud ;

   iii. La détérioration de la qualité de service et les perturbations dues à la fourniture inadéquate des services par le fournisseur Cloud ;

   iv. Les risques et incidents significatifs découlant de la fourniture des services Cloud ;

b. L'analyse d'impact sur l'activité, proportionnée aux risques des processus, services et activités externalisés dans le Cloud ;

c. Les plans de sortie documentés et suffisamment testés prenant en compte les éventuels coûts et impacts ;

d. L'identification de solutions alternatives et l'élaboration de plans de transition pour permettre à l'établissement de transférer ses processus, services et activités externalisés dans le Cloud vers un autre fournisseur de service ou à l'établissement.

Article 15

L'établissement doit tenir compte du principe de la proportionnalité dans le cadre de l'application des prérequis préalables à toute externalisation vers le Cloud en établissant une distinction entre les services Cloud à haut risque et ceux à faible risque. Les services Cloud à haut risque impliquant une délocalisation auprès de FSC basés à l'étranger et des systèmes d'enregistrement qui conservent des informations sensibles ou essentielles, pour respecter les engagements de l'établissement envers les clients et ses contreparties, doivent être soumis à des exigences plus contraignantes que les services Cloud à faible risque qui n'impliquent pas des FSC basés à l'étranger ou d'activités exercées dans d'autres juridictions.

TITRE III : Dispositions contractuelles spécifiques à l'externalisation vers le Cloud

Article 16

Dans le cadre du contrat d'externalisation vers le Cloud, l'établissement définit, à minima, les rôles des parties contractantes à travers des clauses relatives :

a. aux rôles et responsabilités du FSC dans le cadre de la gestion des incidents et des changements ;

b. à la communication du FSC de la survenance de toute faille de sécurité ayant des conséquences directes ou indirectes sur les services Cloud dans des délais raisonnables définis dans le contrat selon la nature et la criticité de l'incident ;

c. à la notification par le FSC de toute modification des conditions d'externalisation convenues préalablement avec l'établissement.

d. A l'information par le FSC de la liste de sous-traitants et de nouvelle toute externalisation de ses fonctions.

Article 17

Dans le cadre du contrat d'externalisation, l'établissement définit ses exigences de services et les modalités de suivi des prestations fournies. Le contrat doit inclure, à minima, des clauses relatives aux :

a. obligations du FSC à répondre aux exigences de confidentialité, d'intégrité et de disponibilité des données de l'établissement ;

b. modalités de suivi et de contrôle des services fournis ;

c. indicateurs clés de performance (KPI) de suivi du dispositif d'externalisation vers le Cloud du FSC. Ces indicateurs doivent refléter la qualité des prestations rendues et faire l'objet d'évaluation périodique à fréquence définie;

d. engagements de service (SLA) du FSC. Des critères d'évaluation des impacts des changements ou des incidents sur les SLA doivent être définis dans le cadre du contrat ;

e. pénalités applicables en cas de non-respect des engagements de service (SLA) définis.

Article 18

L'établissement veille à ce que le contrat d'externalisation vers le Cloud permette d'assurer la sécurité des données hébergées, tout au long de leur cycle de vie. Aussi, ce contrat doit inclure, à minima, les engagements ci-dessous :

a. L'utilisation par le FSC des données de l'établissement aux seules fins de service conformément aux conditions du contrat ;

b. L'application des procédures de récupération et de suppression des données hébergées dans le cadre du contrat ;

c. Les dispositions spécifiques aux plans de continuité d'activité du FSC validés et testés régulièrement ;

d. Les dispositions à mettre en œuvre par le FSC pour garantir la traçabilité des actions effectuées sur les données hébergées ;

e. Les mesures de sécurité, adaptées à la classification des données hébergées, à appliquer par le FSC ;

f. La durée de conservation des données hébergées par le FSC au regard des finalités pour lesquelles elles étaient collectées et en tout état de cause de leur non conservation au-delà de la durée du contrat.

g. Le respect des dispositions de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel notamment en matière de transfert des données à l'étranger.

Article 19

L'établissement veille à ce que le contrat d'externalisation vers le Cloud préserve ses droits à travers des clauses :

a. donnant à l'établissement, à Bank Al-Maghrib et à toute autre entité désignée par ses soins le droit d'effectuer des vérifications sur place ou à distance .

b. Prévoyant la mise à disposition sans restriction par le FSC des droits d'accès aux documents et à son personnel pour effectuer ces vérifications.

c. Prévoyant que le coût de ces vérifications est pris en charge par le prestataire de services au cas où ce dernier ne se serait pas conformé aux dispositions contractuelles.

d. donnant à l'établissement le droit de demander les rapports d'audit réalisés par le FSC et ses sous-traitants;

e. définissant les conditions de réversibilité et modalités de récupération des données de l'établissement à l'issue du contrat. Ces clauses doivent également prévoir des dispositions régissant la destruction des données conformément à la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Les vérifications menées par l'établissement ou toute autre entité désignée par lui couvrent notamment la solidité financière, la conformité juridique, réglementaire et contractuelle, les dispositifs de la gestion et de contrôle mis en place, y compris l'élaboration de rapports réguliers, le processus de gestion du cycle de vie des actifs informatiques, la gestion de la sécurité informatique, de la continuité des activités et de la reprise après sinistre.

TITRE IV : Suivi des fonctions externalisées vers le Cloud

Article 20

L'établissement s'assure de la sécurité des fonctions externalisées vers le cloud à travers la réalisation de tests d'intrusion conformément à la réglementation en la matière. Les résultats des tests d'intrusion doivent être communiqués à Bank Al-Maghrib.

Article 21

L'établissement tient à jour un registre des informations relatives aux fonctions externalisées vers le Cloud. Le registre doit contenir pour chaque fonction, à minima, les informations ci-après :

a. Les dates de début ou de renouvellement du contrat liant l'établissement au FSC et la durée de préavis prévue ;

b. Les législations applicables à l'accord d'externalisation vers le Cloud ;

c. La description des fonctions externalisées vers le Cloud ;

d. Le nom du FSC, le siège social et autres coordonnées pertinentes du FSC ;

e. Les certifications et homologations dont dispose le FSC ;

f. Le(s) pays au sein duquel(desquels) le service sera exécuté, y compris la localisation des données (pays / région) ;

g. L'ensemble des données et systèmes associés aux fonctions externalisées vers le Cloud ;

h. La classification des données externalisées selon l'analyse des risques effectuée préalablement par l'établissement ;

i. Les types de services et modèles de déploiement Cloud mis en place ;

j. Les résultats et la date de la plus récente évaluation des risques réalisée ;

k. La date des derniers audits et des prochains audits prévus, le cas échéant ;

l. Le détail des incidents survenus impactant la sécurité des données ou la disponibilité du service (description de l'incident, date de survenance/résolution, risques, causes, plan d'action ...) ;

m.L'attribution de compétence à une juridiction en cas litige.

Ces informations doivent être retracées annuellement dans le rapport sur le dispositif de contrôle interne adressé à Bank Al-Maghrib.

Article 22

L'établissement qui recourt à l'externalisation vers le cloud, doit notifier auprès de la Commission Nationale de contrôle de la protection des Données à caractère Personnel l'ensemble des traitements de données à caractère personnel concernés par cette externalisation.

Cette notification doit être opérée via le régime prévu par cette commission et accompagnée de(s) demande(s) de transfert y afférente(s).

Titre V : Autres dispositions

Article 23

L'établissement doit identifier, évaluer et gérer les conflits d'intérêts liés à ses opérations / activités de recours au Cloud. Il doit en particulier s'assurer que tout membre de l'organe de direction n'est pas en situation de conflit d'intérêt directe ou indirecte avec le FSC ou avec chaque sous-traitant.

Article 24

Pour les fonctions externalisées vers le Cloud avant la prise d'effet de la présente directive, l'établissement doit s'y conformer dans un délai de 12 mois suivant la date de sa signature.

Article 25

Les dispositions de la présente directive prennent effet à compter de la date de sa signature.

Signé :
Abdellatif JOUAHRI