Position de CACEIS au sujet du règlement général sur le traitement des données (UE) 2016/679 (« RGPD »)

Résumé des traitements de données effectués :	CACEIS Investor services est une banque d'actifs, spécialisée dans les fonctions post-marché liées à l'administration et au suivi de toutes les classes d'actifs. Grâce à une infrastructure informatique solide, nous fournissons des services d'exécution, de compensation, de conservation, de dépositaire et d'évaluation d'actifs sur les marchés du monde entier pour aider les clients institutionnels et les entreprises à atteindre leurs objectifs de développement commercial. Elle est une société réglementée et à ce titre répond aux exigences légales et réglementaires nationales, européennes et internationales.

Table des matières

1 Aperçu des données traitées par CACEIS (RGPD Chapitres 1 et 2)

CACEIS fournit : (a) une gamme de services de marché à ses clients institutionnels allant de l'exécution, de la compensation, de la gestion des transactions, de la tenue de positions, des services de change, de conservation et de trésorerie, de l'administration de portefeuille, des services de données de référence, etc. ; (b) des services sur mesure pour les besoins spécifiques des gestionnaires d'actifs, des institutions, des banques d'affaires, des courtiers et des fonds de capital-investissement, y compris le fiduciaire, la structuration des fonds, la distribution des fonds, les assemblées générales, le dépositaire et le maintien des positions, etc.; (c) des services numériques pour gérer vos données.

Pour réaliser et fournir ces services, CACEIS se conforme non seulement aux normes et directives techniques, mais veille également au respect des réglementations nationales et internationales relatives aux prestataires de services bancaires et d'investissement au sein de l'UE et d'ailleurs.

Les informations sont donc collectées et traitées pour répondre à ces exigences. Les données personnelles sont collectées et utilisées à des fins légales et réglementaires, notamment pour l'exécution des contrats. Seules les données nécessaires sont collectées, traitées puis archivées pour répondre aux exigences de conservation stipulées. Les données ne sont jamais utilisées à d'autres fins.

CACEIS se considère généralement comme le « responsable du traitement » des services fournis à ses clients.

Les données personnelles collectées, stockées et utilisées comprennent :

- Données de personnes physiques agissant en tant que représentants des clients de CACEIS et de leurs investisseurs ;
- Données de personnes physiques agissant en tant que représentants des prospects de CACEIS ;
- Données de tiers qui nous sont confiées par nos clients.

À l'exception de quelques rares traitements, CACEIS ne traite aucune catégorie particulière (art. 9) de données personnelles sauf sur la base d'obligations réglementaires.

2 Respect des droits individuels des personnes concernées (RGPD chapitre 4)

Les « droits » individuels des personnes concernées sont assurés, protégés et garantis par la mise en œuvre des politiques et procédures internes de CACEIS, qui sont régies, contrôlées et évaluées par le Délégué à la Protection des Données.

Les données personnelles traitées par CACEIS sont, soit fournies par les clients à des fins contractuelles ou réglementaires, soit collectées directement par CACEIS pour des raisons légales ou réglementaires. Les données personnelles obtenues dans le cadre d'une relation « Business to Business » sont utilisées uniquement dans le but de respecter les engagements contractuels convenus et, de répondre aux contraintes réglementaires et juridiques nationales et internationales des produits financiers, des marchés et des services d'investissement. Les données personnelles sont donc conservées et archivées à ces fins.

CACEIS n'effectue pas de profilage fondé sur des données à caractère personnel. Quant au traitements réalisés aux fins de lutte contre le blanchiment (AML) et la connaissance des clients, bénéficiaires réels, investisseurs (ou « KYC »), les informations personnelles peuvent être partagées avec les autorités sur demande (par ex. ACPR, BCE, et des autorités de protection des données).

Toutes les demandes reçues par CACEIS seront traitées conformément à la réglementation applicable. Les modalités d'exercice de ces droits sont décrits dans les notices de confidentialité de CACEIS, également disponibles sur le site Internet de CACEIS : **https://www.caceis.com/who-we-are/compliance /**

Les droits des personnes concernées sont les suivants :

- Droit à l'information de base
- Droit d'accès
- Droit de rectification
- Droit à l'effacement et « droit à l'oubli »
- Le droit de restreindre le traitement
- Droit d'opposition au traitement

3 Dispositif de CACEIS pour l'application du Règlement Général sur la Protection des Données

3.1 CONFIGURATION JURIDIQUE DE CACEIS

CACEIS a défini la stratégie, son organisation interne et ses procédures à l'échelle du groupe pour mettre en œuvre le RGPD en termes contractuels et juridiques envers les clients, les fournisseurs, les contreparties, les personnes concernées et les échanges intra-groupe.

L'objet est de définir le cadre contractuel et juridique que toutes les entités et succursales du groupe CACEIS auront en place avec les tiers (clients, fournisseurs et contreparties), les personnes concernées ainsi qu'entre les entités et succursales du groupe en matière de protection des données personnelles afin de mettre en œuvre les exigences du RGPD.

3.2 QUALIFICATION DU RÔLE DE CACEIS VIS-A-VIS DU RGPD

Les définitions de contrôleur et de sous-traitant sont les suivantes :

Responsable du traitement ou responsable du traitement	Conformément à l'art. 4 (7) du RGPD, la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, **détermine les finalités et les moyens du traitement des données personnelles** ; lorsque les finalités et les moyens d'un tel traitement sont déterminés par le droit de l'Union européenne ou d'un État membre, le responsable du traitement ou les critères spécifiques pour sa nomination peuvent être prévus par le droit de l'Union européenne ou d'un État membre.

Sous-traitant ou sous-traitant	Conformément à l'art. 4 (8) du RGPD, une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite des données personnelles **pour le compte du responsable du traitement.**

3.2.1 Qualification de CACEIS au RGPD vis-à-vis de ses clients

Lorsque CACEIS fournit des services à ses clients, ceux-ci sont rendus d'une part, dans le respect de toutes les réglementations et obligations imposées à CACEIS (y compris les durées de conservation des données personnelles) ; d'autre part, en faisant bénéficier ses clients de services industrialisés avec toutes les compétences nécessaires. Cela amène donc CACEIS à fixer lui-même les finalités et les moyens des traitements effectués pour ses clients. Par conséquent, CACEIS doit être qualifié de « Responsable de traitement » conformément aux lignes directrices 07/2020 du Comité européen de la protection des données (« EDPB ») sur les notions de responsable de traitement et de sous-traitant dans le RGPD.

Néanmoins, si un traitement particulier devait être identifié par un client comme étant traité par CACEIS en qualité de sous-traitant, le client agissant en qualité de Responsable de traitement (selon les critères de l'EDPB), les instructions du client concernant un tel traitement devra être fourni par écrit à

CACEIS, dans un document contractuel, à convenir avec CACEIS. Ce document devra comporter toutes les caractéristiques requises, conformément à l'article 28.3 du RGPD (objet, durée, nature et finalité du traitement, type de données personnelles et catégories de données et sujets auprès desquels le traitement des données personnelles est réalisé par CACEIS pour le compte du client).

Le tableau ci-dessous donne des exemples de caractéristiques des traitements réalisés par CACEIS :

Services pour lesquels des traitements pourraient être effectués par CACEIS	Objet, nature et finalité du traitement	Catégories de personnes concernées	Type de données personnelles	Base juridique du traitement des données personnelles	Durée du traitement	Positionnement de CACEIS	Commentaires
Banque dépositaire/fiduciaire (fonction de dépositaire, conservation des actifs et détention de positions)	• Contrôle de la régularité des décisions d'investissement et suivi des ratios réglementaires Conservation des actifs du fonds (tenue de comptabilité pour les actifs financiers et tenue de position pour les actifs non financiers)	Investisseurs	Identifiants, état civil, etc...	Exécution du contrat	Le traitement se poursuivra pendant la durée du contrat de service concerné, et par la suite, sans que les données personnelles soient conservées plus longtemps que nécessaire en vertu de la loi applicable.	Responsable de traitement	

Custody	• Traitement du règlement/livraison • Traitement des actions de l'entreprise sur les positions empruntées ou les positions d'achat/vente • Déclaration fiscale • Traitement des assemblées générales	Clients, investisseurs	Informations d'identification, informations fiscales	Exécution du contrat	Le traitement se poursuivra pendant la durée du contrat de service concerné, et par la suite, sans que les données personnelles soient conservées plus longtemps que nécessaire en vertu de la loi applicable.	Responsable de traitement	
Administration et comptabilité des actifs : reporting réglementaire	Production de rapports réglementaires pour le compte de clients (fonds, sociétés de gestion, gestionnaires d'investissement ou compagnies d'assurance) conformément à la convention de service concernée	Investisseurs	Selon l'étendue de la prestation, les coordonnées personnelles ou professionnelles (Nom, prénom, adresse email, numéros de téléphone, coordonnées bancaires) nécessaires à l'exécution de la prestation.	légitime , exécution du contrat, obligation légale	Le traitement se poursuivra pendant la durée du contrat de service concerné, et par la suite, sans que les données personnelles soient conservées plus longtemps que nécessaire en vertu de la loi applicable.	Responsable de traitement	CACEIS agit pour le compte de ses clients mais se conforme aux obligations réglementaires ou législatives

Due diligence, AML/KYC pour le compte des clients, traitement des ordres des investisseurs et/ou gestion de l'information	Traitement les données personnelles des investisseurs des clients conformément à la réglementation AML/KYC applicable et au contrat de service correspondant	Les investisseurs et leurs bénéficiaires effectifs	Nom, date de naissance, adresses postale et électronique, numéros d'identification du passeport, numéros de téléphone, numéros de compte bancaire et informations financières pour la vérification de la source de richesse et de la source des fonds, et éventuellement certaines catégories spéciales de données personnelles.	légitime , exécution du contrat, obligation légale	Le traitement se poursuivra pendant la durée du contrat de service concerné, et par la suite, sans que les données personnelles soient conservées plus longtemps que nécessaire en vertu de la loi applicable.	Responsable de traitement	CACEIS y répond à ses propres obligations réglementaires ; ces obligations sont partagées avec le client ; ni les clients ni CACEIS n'ont la possibilité de modifier le traitement concernant le KYC/AML ni le type de données personnelles à collecter. Aucune instruction documentée ne peut être donnée par les clients à CACEIS pour procéder à ce traitement.

Services liés à la Distribution : Transfert agent, Agent Payeur, PTA (prime transfer agent), RNI, Routage d'Ordres, Négociation, Suivi des ordres des investisseurs et/ou informations sur les réseaux de distribution. Le cas échéant, tenue locale du registre des actionnaires ou des porteurs de parts.	Traitement lié à la distribution locale et/ou à la distribution transfrontalière conformément au contrat de service concerné	Investisseurs	Données personnelles ou professionnelles (Nom, prénom, adresse email, numéros de téléphone, coordonnées bancaires) nécessaires à l'exécution de la prestation et éventuellement certaines catégories particulières de données personnelles	légitime , exécution du contrat, obligation légale	Le traitement se poursuivra pendant la durée du contrat de service concerné, et par la suite, sans que les données personnelles soient conservées plus longtemps que nécessaire en vertu de la loi applicable.	Responsable de traitement	CACEIS agit dans le respect des lois et règlements, il s'agit d'une opération de transformation industrielle sans personnalisation

Domiciliation de fonds et secrétariat social de fonds : Notamment, assistance apportée aux assemblées générales d'actionnaires et conseil d'administration.	Inscription des données personnelles des dirigeants de fonds au Registre du Commerce. Assurer le secrétariat de la société lors des assemblées générales et réunions du conseil d'administration et services de secrétariat associés conformément au contrat de service pertinent	Administrateurs de fonds, investisseurs et, le cas échéant, gestionnaires de placements, propriétaires véritables	Données personnelles ou professionnelles (Nom, prénom, adresse email, numéros de téléphone, éventuellement coordonnées bancaires) nécessaires à l'exécution de la prestation et éventuellement certaines catégories particulières de données personnelles	légitime , exécution du contrat, obligation légale	Le traitement se poursuivra pendant la durée du contrat de service concerné, et par la suite, sans que les données personnelles soient conservées plus longtemps que nécessaire en vertu de la loi applicable.	Responsable de traitement	Aucune instruction directement documentée n'est reçue du client concernant le traitement des données personnelles ou des données personnelles. L'équipe de domiciliation ne traite les données personnelles que conformément à la réglementation locale applicable ou à l'intérêt légitime d'exercer le service.

Custody Network (fait partie des services de custody)	Fournir les données personnelles des investisseurs et des bénéficiaires effectifs aux sous-dépositaires lorsque le marché local ou la loi applicable l'exigent	Les investisseurs et leurs bénéficiaires effectifs	Nom, date de naissance, adresses postale et électronique, numéros d'identification du passeport, numéros de téléphone, numéros de compte bancaire et informations financières pour la vérification de la source de richesse et de la source des fonds, et éventuellement certaines catégories spéciales de données personnelles.	Intérêt légitime à gérer le service, légal obligation conformément à la législation locale applicable.	Le traitement se poursuivra autant que nécessaire dans le respect de la réglementation locale.	Responsable de traitement	

Private Equity, Immobilier & Titrisation : Administration de fonds	Instructions de caisse / Tenue de registre/Constituer ou mettre à jour et contrôler le KYC des investisseurs	Investisseurs, tiers (locataires)	Données personnelles ou professionnelles (Nom, prénom, adresse email, numéros de téléphone, coordonnées bancaires) nécessaires à l'exécution de la prestation	Intérêt légitime, obligation légale	Le traitement se poursuivra pendant la durée du contrat de service concerné, et par la suite, les données personnelles ne seront pas conservées plus longtemps que nécessaire conformément à la réglementation locale.	Responsable de traitement	
Communication multi-canal : OLIS, OLIS MOBILE, SWIFT & autres formats, TEEPI (Tailored Electronic Exchange Platform for Investors)	Portail internet unique pour tous nos services clients ; service de mobilité pour les informations essentielles aux gestionnaires d'actifs (suivi et validation VL, suivi en temps réel des investisseurs) ; solutions de connexion multiservices via la messagerie SWIFT ; réseau d'échange de données pour les relations entre établissements financiers et sociétés de gestion	Investisseurs utilisateurs Il peut s'agir de dirigeants d'institutions financières et de sociétés de gestion	Données personnelles ou professionnelles (Nom, prénom, adresse email, numéros de téléphone, coordonnées bancaires) nécessaires à l'exécution de la prestation	Intérêt légitime, exécution du contrat pour les clients, obligation légale		Responsable de traitement	

Lors de l'externalisation de services auprès de fournisseurs, le fournisseur est généralement qualifié de sous-traitant de CACEIS pour le traitement des données personnelles dans le cadre de la prestation externalisée et sous réserve des instructions de CACEIS (que CACEIS soit responsable du traitement ou sous-traitant des données personnelles vis-à-vis d'un client).

CACEIS utilise des clauses types pour toute relation contractuelle avec ses fournisseurs. L'objectif de ces clauses est de garantir que le fournisseur effectue tout traitement de données personnelles conformément au RGPD et de fournir des instructions pertinentes à cet égard.

Certaines autres situations spécifiques peuvent nécessiter une analyse plus approfondie de la qualification et de l'ajustement du cadre contractuel. C'est le cas notamment des relations avec les consultants, les sous-conservateurs et les contreparties financières.

Dans tous les cas, un accord contractuel sera conclu entre les parties pour fixer la qualification, définir les obligations respectives et convenir du flux de communication ou des actions entre les parties afin de se conformer au RGPD.

4 Mesures de sécurité organisationnelle

4.1 Délégué à la protection des données (RGPD chapitre 4, section 4, articles 37, 38, 39)

Le groupe CACEIS a désigné un DPO pour l'ensemble des entités qui le constitue. Les détails sont disponibles via les sites Internet de l'entreprise. Le DPO est directement rattaché au Chief Compliance Officer de CACEIS, membre du Comité Exécutif. Le DPO est en charge de la protection des données à caractère personnel du groupe et coordonnera un réseau de correspondants en matière de protection des données au niveau des sites et des entités.

Le DPO de CACEIS est joignable par email : caceisdpo@caceis.com

4.2 Engagement envers le secret et la confidentialité des données (RGPD Chapitre 4, Section 2, Article 32.1)

Tous les collaborateurs de CACEIS sont tenus au respect du secret informatique, bancaire, du secret des affaires et de la confidentialité. Ceci, dans le cadre et dans les limites du droit national du travail (par exemple contractuel, charte d'entreprise, lettres d'engagement, ...). Cet engagement comprend une obligation de confidentialité après la rupture ou le changement du contrat de travail.

Le Passeport Sécurité de l'Information CACEIS est un guide délivré aux collaborateurs pour leur présenter les bonnes pratiques à mettre en œuvre dans l'exercice de leurs activités professionnelles. Il s'inscrit pleinement dans les procédures et bonnes pratiques du Crédit Agricole.

4.3 Directives de travail, séances de coaching et de formation sur la protection des données (RGPD Chapitre 4, Section 4, Article 39.1(b))

CACEIS publie et maintien des politiques et des lignes directrices en matière de **confidentialité** et **de protection des données personnelles** . La politique de protection des données et de sécurité de l'information du groupe CACEIS impose à toutes les entités de veiller au respect des exigences légales nationales et internationales. Par ailleurs, CACEIS a publié une Charte RH spécifique pour la protection des informations personnelles identifiables (IPI) des salariés.

Pour garantir le développement personnel et la sensibilisation permanente des employés, nous utilisons des plateformes de formation conformes aux normes de l'industrie afin de fournir un contenu mis à jour régulièrement afin de permettre au personnel de gérer lui-même son développement tout au long de sa carrière. Des campagnes de sensibilisation aux pratiques réglementaires et industrielles sont dispensées aux collaborateurs de CACEIS via des ateliers, des sessions de questions-réponses et de e-learning.

L'inscription aux formations et la participation aux cours de formation sont gérées et suivies par la DRH.

4.4 Registres des activités de traitement (RGPD, chapitre 4, section 1, article 30)

CACEIS entretien un registre des traitements de Données Personnelles au sens de l'article 30 du RGPD.

Des procédures, des processus et des politiques internes (notamment la gouvernance des projets, le recueil d'accords pour le lancement de nouveaux produits ou la modification de produits existants, l'obligation de conduire des études de risque pour tout nouveau traitement informatique ou la modification substantielle de traitement informatique), une revue annuelle obligatoire du registre des traitements, garanti à CACEIS de disposer d'un registre exhaustif et à jour.

Pour chaque traitements, le registre contient les informations suivantes :

- L'entité et le responsable du traitement,
- Les prestataires externes éventuels,
- La liste des informations personnelles traitées,
- Identifier les transferts d'informations personnelles hors de CACEIS (vers le groupe Crédit Agricole / hors groupe Crédit Agricole, au sein de l'UE),
- D'identifier, lorsqu'ils existent, les transferts informations personnelles hors de l'UE et la manière dont ces transferts sont sécurisés,
- Les principales mesures de protection des données.

Le DPO supervise le Registre des traitements et le respect de la réglementation. Le responsable du traitement et ses représentants sont tenus responsables de garantir que les informations du Registre sont correctes et maintenues à jour.

4.5 Procédures en cas de violation de données personnelles (RGPD Section 2, articles 33 et 34)

CACEIS considère avec sérieux toutes les violations de données, quelle que soit leur nature. Le risque de violation des données personnelles est examiné et des mesures appropriées sont prises pour atténuer ces risques. Les violations de données sont gérées sur la base de politiques et directives internes associées à la gestion de crise.

Sous la direction du DPO de CACEIS, la documentation pertinente (politique, lignes directrices) a été mise à jour en coordination avec le Groupe Crédit Agricole. Des lignes directrices du groupe ont été émises et intégrées.

Par défaut, après détection, si la gravité et la portée de l'incident concernant des Données personnelles le justifie, le DPO de CACEIS, le RSSI de CACEIS et le DPO Groupe Crédit Agricole interviennent afin d'évaluer et de coordonner la gestion de l'incident et les réponses adaptées. Le plan d'action sera naturellement escaladé et notifié aux DPO de toutes les parties impactées si nécessaire et selon les accords contractuels convenus.

En fonction de la gravité de l'impact sur les droits et libertés des personnes physiques, et conformément à l'article 33 du RGPD, le DPO CACEIS notifiera l'Autorité de Protection des Données (DPA) dont dépend le groupe CACEIS et, se chargera d'informer, le cas échéant, les personnes concernées. Sauf, bien

sûr, si le contrat signé avec ses clients indique que CACEIS agit en qualité de « sous-traitant » et, dans ce cas, CACEIS ne notifiera pas directement les personnes concernées qui restent sous la responsabilité du client en tant que « responsable du traitement » (article 34 du RGPD).

CACEIS attend et a pris des mesures pour que les sous-traitants notifient à CACEIS toute violation de données à caractère personnel dans un délai prédéfini et sans retard indu.

4.6 Lignes directrices sur la sécurité de l'information (chapitre 2, article 6 ; chapitre 4, section 2, articles 24, 25 ; et section 3, article 35)

La sécurité du système d'information est régie par la politique de sécurité de l'information de CACEIS (une version est disponible sur le site Internet de CACEIS) et elle est renforcée par des directives spécialisées et des procédures opérationnelles particulières. Celles-ci couvrent les principaux thèmes tels que la classification, les rôles et responsabilités, la gestion des utilisateurs et le contrôle d'accès, la sécurité de l'infrastructure, les postes de travail des utilisateurs, y compris les ordinateurs de bureau et les systèmes mobiles, les normes de développement, les sauvegardes de données, etc. Ceux-ci sont régulièrement revus et mis à jour pour tenir compte de l'évolution des technologies et des risques.

Le passeport de sécurité de l'information de CACEIS est une directive destinée à tous les employés qui décrit les bonnes pratiques à utiliser dans l'exercice de leurs fonctions. Il est parfaitement aligné sur les procédures et les bonnes pratiques du Crédit Agricole.

Des évaluations de risques sont effectuées pour toutes les nouveaux traitements et pour tous les changements importants apportés aux traitements existants. TUNES, la méthode d'évaluation des risques de CACEIS, est obligatoire pour tous les nouveaux traitements de données à caractère personnel afin de respecter les obligations de « privacy by design » et de « privacy by default » définies par le RGPD. Lorsque le type d'activité du traitement présente des risques élevés pour les droits et libertés des personnes physiques, une étude d'impact sur la protection des données (DPIA) est réalisée (article 35 du RGPD). La méthodologie des DPIA est entièrement alignée sur celle du Groupe Crédit Agricole.

Les systèmes de CACEIS sont conçus et intègrent par défaut des mesures de protection et, de par leur conception, ces mesures comprennent certaines de celles décrites ci-dessus. Par défaut, il n'y a pas d'accès possibles aux données. Conformément à l'article 25 du RGPD, certaines lignes directrices existantes en matière de sécurité pourront être renforcées afin de réduire encore les risques pour les droits et libertés des personnes physiques, en particulier pour des catégories particulières de données.

En ce qui concerne le développement de logiciels et de systèmes, une politique spécifique porte sur l'acquisition, le développement et la maintenance et couvre les sujets suivants :

- intégration de la sécurité dans les projets
- analyse des risques et exigences en matière de sécurité
- conception et mise en œuvre des solutions de sécurité
- tests, recette fonctionnelle et mise en production

- documentation
- maintenance
- intégration de la sécurité dans les développements

De plus, diverses procédures et normes sont en place, dont :

- MESARI qui est utilisé pour l'évaluation des risques.
- SECAPI qui est une norme du groupe CASA qui fournit des principes de confidentialité dès la conception.
- Des procédures opérationnelles normalisées (SOP) sont en place au sein du service informatique.

Le développement, la mise en œuvre et la maintenance des logiciels sont documentés et assurent le maintien des procédures opérationnelles. La documentation utilise les bonnes pratiques et des normes de l'industrie comme COBIT et ITIL.

4.7 Stockage/traitement des données en dehors de l'Europe (RGPD chapitre 5, article 44)

Toutes les données personnelles sont stockées et traitées dans les Data Center de CACEIS situés en Europe. Pour certaines activités, qui concernent principalement l'administration de fonds et la comptabilité, une petite quantité de traitement se fait à distance à partir des bureaux de CACEIS situés à Hong Kong ou au Canada.

Certaines activités de traitement font appel à des tiers, comme le développement et la maintenance de logiciels. L'activité est réalisée à distance sur des systèmes dans des Data Centers européens et utilise des données anonymisées.

5 Mesures techniques de sécurité pour protéger les données personnelles

5.1 Aperçu de l'architecture technique

Les services informatiques de CACEIS sont principalement axés sur la conception, la construction et l'exploitation de systèmes d'information hautement automatisés. Les systèmes exploitent des technologies telles que des systèmes centraux (Mainframe), Microsoft Windows, Linux, les bases de données Oracle et les middlewares Web.

L'hébergement de la plateforme technique et la gestion opérationnelle des productions, sont externalisés à DXC et situés au Luxembourg. Les services liés aux postes de travail sont gérés et fournis par Crédit Agricole CAGIP avec des Data Centers situés en France.

5.2 Mesures de pseudonymisation et d'anonymisation des données personnelles (RGPD, chapitre 4, section 2, article 32.1(a))

La politique de sécurité de l'information de CACEIS stipule qu'aucune donnée de production ne doit être disponible dans les environnements de non-production (développement, test, etc.) à moins d'être entièrement anonymisée. Cette règle s'applique aussi aux données personnelles.

5.3 Mesures de cryptage des données personnelles (RGPD Chapitre 4, Section 2, Article 32.1(a))

Les mesures suivantes sont en place :

1. Les ordinateurs mobiles (laptops) sont équipés de technologies de chiffrement du disque dur
2. Le protocole de sécurité TLS a été mis en œuvre pour l'échange de courriels
3. Le protocole de sécurité HTTPS est utilisé pour sécuriser l'accès aux applications Web
4. Les transferts de données avec les clients sont cryptés
5. Une solution est disponible pour chiffrer les courriels sensibles

5.4 Mesures visant à garantir une confidentialité continue (RGPD, chapitre 4, section 2, article 32.1(b))

Les mesures suivantes sont en place :

1. Les bâtiments et les zones extérieures sont contrôlés par le personnel de sécurité. Des alarmes sont en place. Les entrées sont protégées par des contrôles d'accès techniques (contrôle d'entrée et contrôle vidéo) et des mesures organisationnelles (réception)
2. Identification et revues appropriées des utilisateurs et des administrateurs accédant aux données personnelles
3. Mise en œuvre d'une politique sur les mots de passe

4. Verrouillage de l'écran après la période d'inactivité
5. Infrastructure réseau sécurisée
6. Les ports USB sont bloqués par défaut
7. L'accès aux données personnelles par des personnes non autorisées est empêché
8. Transport physique sécurisé
9. L'élimination, des supports de stockage de données des PC usagés et des impressions est contrôlée
10. Déploiement d'une solution d'impression sécurisée

5.5 Mesures visant à garantir l'intégrité continue des données (RGPD, chapitre 4, section 2, article 32.1(b))

Les mesures suivantes sont en place :

1. Le principe de l'identifiant unique des utilisateurs est en place
2. Les droits d'accès à haut privilège sont séparés des activités commerciales et doivent être liés à un utilisateur identifié
3. La transmission des données physiques est consignée et confirmée
4. La transmission électronique des données est enregistrée et contrôlée
5. Selon l'analyse des risques, la saisie des données pour certaines applications à haut risque n'est possible qu'avec un principe de contrôle à 4 yeux.
6. L'accès aux données personnelles est surveillé et enregistré
7. Les activités des administrateurs des systèmes et des données sont tracées

5.6 Mesures pour garantir une disponibilité continue (RGPD Chapitre 4, Section 2, Article 32.1(b)(c))

Les mesures suivantes sont en place :

1. Des SLA sont en place avec les fournisseurs
2. Installations sécurisées contre les cambriolages, les incendies, les inondations, la chaleur et les pannes d'électricité
3. Des centres de sauvegarde des données et des procédures sont en place pour rétablir la disponibilité des données personnelles en temps opportun
4. Le rétablissement et la restauration sont testés
5. Les concepts de BCP (Business Continuity Plan) ont été conçus et mis en œuvre.
6. Des scénarios spécifiques ont été élaborés pour couvrir des incidents à haut risque tels que des incidents liés aux personnes (virus, inondations, …) et technique (panne massive des postes de travail, défaillance logique des Data Centers causée par une erreur humaine, défaillance technique ou cyber menaces).

7. Tests réguliers des PCA (Plan de Continuité d'Activité) pour s'assurer que les systèmes et les processus sont entièrement opérationnels et à jour.

5.7 Mesures visant à garantir la résilience continue des systèmes et des services (RGPD, chapitre 4, section 2, article 32.1(b))

Les mesures suivantes sont en place :

1. Chaque demande fait l'objet d'une évaluation des risques qui dressent la carte des contrôles de sécurité et des mesures de sécurité appropriés. Les logiciels d'application sont soumis aux normes internes d'architecture de sécurité SECAPI fixant les règles de développement et de maintenance. Ils sont testés et validés avant que le contrôle des changements ne permette leur promotion dans les environnements de production.
2. Le test DRP et des tests de pénétration sont effectués pour garantir la robustesse de l'environnement de traitement des données.
3. Une analyse de sécurité régulière du réseau où l'équipement est rattaché, du logiciel utilisé et de toute vulnérabilité. Des plans de remédiation sont élaborés pour les éléments identifiés, hautement prioritaires.
4. La solution de « Threat intelligence » est utilisée pour évaluer et analyser les niveaux de risque et les menaces.
5. Installations sécurisées contre le vol, les incendies, les inondations, la chaleur et l'alimentation électrique d'urgence dans les zones matérielles.
6. Des procédures de sauvegarde des données sont en place pour restaurer la disponibilité des données personnelles en temps opportun.
7. La récupération et la restauration des données sont testées.

5.8 Mesures pour l'examen, l'évaluation et l'évaluation réguliers de l'efficacité des mesures techniques et organisationnelles (RGPD, chapitre 4, section 2, article 32.1(d))

Les mesures suivantes sont en place :

1. Des contrôles internes ont été conçus et mis en œuvre pour surveiller l'efficience et l'efficacité. Il s'agit notamment des contrôles au niveau opérationnel (niveau 1), des contrôles consolidés (niveaux 2 et 2.1) et des contrôles au niveau 3.
2. Les audits sont réalisés en interne et en externe,
3. Tests réguliers des plans de reprise après sinistre et de continuité des activités
4. Le plan de contrôle du RGPD est en cours d'élaboration et sera mis en œuvre en 2018.
5. Les mesures techniques et organisationnelles (MTO) sont régulièrement examinées.

6 Mesures de protection techniques et organisationnelles spécifiques

6.1 Mesures de sécurité physique

6.1.1 Espaces de bureaux CACEIS

Les bâtiments et bureaux de CACEIS sont protégés 24h/24 et 7j/7 grâce à des technologies telles que la vidéosurveillance, la détection d'intrusion et les rondes nocturnes du personnel de sécurité.

L'entrée dans le bâtiment nécessite une autorisation préalable et un titre d'accès. Les badges permettent de restreindre l'accès et la circulation au sein des bâtiments. Tous les salariés reçoivent un badge. Les visiteurs se voient délivrer un titre d'accès temporaire une fois leur identité confirmée et la visite autorisée par un collaborateur de CACEIS.

6.1.2 Installations de traitement des centres de données

Les installations de traitement de CACEIS sont très étroitement contrôlées. CACEIS maintient des procédures formelles d'accès permettant l'accès physique aux centres de données. Les centres de données sont hébergés dans des installations qui nécessitent un accès par carte électronique spécifique et une preuve d'identité. Les listes d'accès sont maintenues et révisées fréquemment. Les datacenters de CACEIS nécessitent des opérations de sécurité sur site chargées de surveiller et d'enregistrer toutes les fonctions physiques de sécurité du datacenter 24h/24 et 7j/7.

6.2 Gestion et contrôle de l'authentification

6.2.1 Identification de l'utilisateur

Des politiques et des procédures sont définies pour garantir que l'identification appropriée des utilisateurs et des administrateurs accédant aux données personnelles est identifiée.

CACEIS dispose d'un système centralisé de gestion des identités et des accès (IAM). Ce système est responsable de l'attribution des identités des utilisateurs, les identités des utilisateurs sont uniques pour tout le personnel souhaitant accéder et utiliser n'importe quelle partie du Système d'Information de CACEIS. L'accès ne peut s'effectuer que via un poste de travail connecté au réseau CACEIS. Ceux-ci nécessitent une identité d'utilisateur personnelle et au minimum un mot de passe. Dans certains cas, des applications spécifiques peuvent nécessiter une identification à deux facteurs.

Les politiques de sécurité des informations du CACES exigent que les privilèges soient séparés et distincts des activités commerciales habituelles. Par conséquent, un identifiant d'utilisateur dédié est attribué aux personnes désignées. Les privilèges incluent des tâches spéciales d'administration du système et des applications.

Pour garantir que l'USER ID reste pertinent, des campagnes de recertification et de conciliation sont régulièrement menées. Ainsi, tous les USER ID orphelins et invalides sont immédiatement désactivés et supprimés si nécessaire (par exemple, désactivation en temps opportun des USER ID des employés qui ont quitté l'entreprise).

6.2.2 Authentification

L'IAM contrôle l'accès aux systèmes de production en fonction de règles définies. CACEIS s'appuie sur des technologies telles que LDAP, Kerberos et un système propriétaire utilisant des clés RSA (ou d'autres clés logiques) pour fournir des mécanismes d'authentification sécurisés et flexibles. Ces mécanismes sont conçus pour accorder uniquement des droits d'accès approuvés. L'authentification auprès des systèmes techniques est en outre contrôlée via une plateforme dédiée.

L'authentification avec CACIS nécessite généralement un mot de passe secret personnel, bien que dans quelques cas, une authentification à deux facteurs soit effectuée à l'aide de cartes à puce et de dispositifs à jetons. Les règles et normes de gestion des mots de passe sont régies par les politiques de sécurité de l'information. Ces normes incluent des restrictions telles que la réutilisation des mots de passe, leur force et leur durée de vie. Les règles de mot de passe suivantes sont implémentées et contrôlées dans le répertoire actif Windows :

- Au moins 12 caractères sont définis dans la politique
- Durée de vie maximale du mot de passe : 90 jours
- Compte verrouillé : après 5 tentatives de connexion

6.2.3 Accès aux systèmes de traitement des données

Tous les systèmes de traitement des données (postes de travail, serveurs, ..) sont connectés par un réseau interne CACEIS. L'accès aux systèmes informatiques n'est possible qu'à partir du réseau CACEIS.

Les standards de conception du réseau CACEIS s'appuient sur les standards du Crédit Agricole qui sont toujours aux meilleurs standards du marché. Le réseau CACEIS est ségrégué physiquement et logiquement (finalité, risque, technologie) intégrant des technologies de sécurité qui surveillent, détectent et préviennent les intrusions (Firewalls, IDS, IPS et WAF). La redondance du système et la tolérance aux pannes font partie de l'architecture du réseau pour garantir que l'accès aux systèmes de traitement des données est conforme aux exigences des SLA commerciaux.

Les paramètres système suivent un principe de « refus par défaut ». Cela signifie que des configurations de pare-feu et de routeur ont été mises en place afin de restreindre le trafic entrant et sortant et que tout ce qui n'est pas explicitement autorisé est interdit. Par défaut, et de par leur conception, ces paramètres refusent tous les flux et communications au-delà des frontières, seuls les flux définis sont autorisés. Un Change Acceptance Board (CAB) est dédié aux flux, protocoles et services réseau. Des contrôles sont mis en place pour contrôler le respect de nos politiques techniques.

Le suivi est effectué en temps réel par le moniteur Crédit Agricole CERT 24h/24 et 7j/7 et CACEIS SOC. En cas d'avertissement ou d'irrégularités, le responsable de la sécurité des technologies de l'information (ITSO) et le SOC lancent des réponses conformément aux procédures convenues.

6.3 Contrôle d'accès par gestion des autorisations

L'attribution des accès est formalisée et régie par la Politique de Contrôle d'Accès de CACEIS (faisant partie des Politiques de Sécurité de l'Information). La procédure opérationnelle standard (SOP) décrit le fonctionnement du processus de gestion, y compris l'autorisation et l'attribution des « Accès ».

L'accès est autorisé uniquement sur la base du besoin d'en connaître. L'autorisation d'accès est effectuée à l'aide d'un flux de travail et est requise à la fois par le gestionnaire et le propriétaire de l'application. Dans certains cas, une approbation supplémentaire peut être requise. L'attribution de droits spécifiques est gérée par l'application et attribuée une fois autorisée par les gestionnaires.

Les workflows de gestion des autorisations sont effectués au sein du système IAM, où la fourniture et l'attribution des droits sont gérées à l'aide de profils métier prédéfinis. Seul le responsable du profil professionnel peut demander une modification du profil professionnel. L'approbation du responsable du profil d'entreprise, du propriétaire de l'application métier et du service des risques est requise pour attribuer un nouvel accès à un profil d'entreprise.

Le système IAM effectue la révocation automatiquement. En complément, des campagnes de recertification sont réalisées régulièrement par le gestionnaire et le propriétaire de l'application pour certifier que le besoin est toujours d'actualité.

Les profils d'entreprise et les droits d'accès associés sont définis pour appliquer les principes du « besoin de savoir », du « moindre privilège » et de la « séparation des tâches ». Des revues sont réalisées avec la direction des risques pour vérifier les combinaisons de droits d'accès toxiques.

6.4 Protection contre la copie des données

La Politique de Sécurité de l'Information de CACEIS définit les règles d'utilisation des médias et de traitement des données. L'utilisation de supports numériques portables n'est pas autorisée. Les ports USB sont bloqués par défaut et les particuliers peuvent demander une activation temporaire sous conditions strictes. Seuls les supports externes agréés par CACEIS peuvent être utilisés pour stocker les données.

6.5 Contrôle de la divulgation

6.5.1 Transport d'informations et transmission électronique de données

Les politiques de sécurité des informations et les SOP définissent des mesures de transport sécurisées pour la protection contre les accès non autorisés et les utilisations abusives.

Le transport physique des informations, en particulier des informations confidentielles et sensibles, est restreint. CACEIS fait appel à des services de transport sécurisés spécifiques.

Transferts électroniques, CACEIS transfère la majorité des informations par voie électronique, via des connexions Internet sécurisées et des transferts de fichiers sécurisés. Chaque expéditeur participant à la transmission est identifié grâce à des signatures électroniques. La transmission de données personnelles sur des réseaux externes utilise une cryptographie solide et des protocoles sécurisés, tels que l'utilisation de TLS, SSH, HTTPS, SFTP, IPSEC. Toutes les transmissions de données électroniques sont enregistrées et surveillées.

Des mesures de sécurité sont mises en œuvre pour surveiller et contrôler le flux de données via les points finaux et les réseaux externes. Ces mesures incluent les technologies de pare-feu, IDS, IPS et WAF. Un Change Acceptance Board est dédié aux revues de flux réseau, de protocoles et de services et aux demandes de plans.

6.5.2 Sécurité des données

Les politiques de sécurité des informations et les SOP de CACEIS définissent notre approche en matière de classification des actifs, y compris les actifs applicatifs et les actifs de données. La majorité des actifs sont inventoriés et classés sur la base d'évaluations des risques qui incluent l'évaluation des axiomes de sécurité de l'information : confidentialité, intégrité et disponibilité. Cette approche inclut la classification des données personnelles. Le processus de classification des actifs est une étape déterminante pour garantir que le choix des mesures et des contrôles de sécurité est effectué en fonction du niveau de criticité de l'actif.

6.5.3 Tests de résilience et de pénétration du système

La résilience et la robustesse des systèmes sont des aspects importants des services fournis par CACEIS. Pour s'assurer qu'elles respectent nos normes commerciales, nous planifions et effectuons de nombreux tests de traitement des données tout au long de l'année. Ces tests comprennent les tests de continuité des activités (BCP) et de reprise après sinistre (DRP) et les tests de pénétration (PEN TEST). Le contrôle des changements fait partie du processus qui contribue à s'assurer que les essais sont effectués correctement avant la livraison des changements dans les environnements de production.

Le DRP consiste à s'assurer que les plans sont documentés, à jour et mis à l'essai pour un certain nombre de scénarios de catastrophe définis. La récupération de données inclut notre capacité à restaurer les informations. Guidés par la politique de sauvegarde qui définit les normes et les pratiques pour la sauvegarde et la récupération d'informations sécurisées, nous effectuons des tests de restauration réguliers.

Les TESTS PEN sont réalisés régulièrement par CACEIS sur nos infrastructures critiques pour tester la force, la robustesse, la résilience, la performance et le maintien de l'étanchéité des systèmes de sécurité déployés. De plus, CACEIS dispose d'un outil de renseignement sur les menaces qui analyse constamment l'état de son système et de son réseau afin de détecter d'éventuelles failles de sécurité.

6.5.4 PC portables (ordinateurs portables) et appareils mobiles

Les mesures de protection pour les PC portables (ordinateurs portables) et les appareils mobiles sont définies par la politique de sécurité des informations et décrites dans les normes et SOP de sécurité des informations. L'utilisation des appareils mobiles (ordinateurs portables, smartphones, tablettes, etc.) est

soumise à des règles particulières. L'utilisateur s'engage à respecter ces règles en signant un document spécifique lors de sa délivrance avec l'appareil concerné.

Les informations sur les ordinateurs portables sont protégées par des technologies de cryptage du disque dur et par d'autres mesures de sécurité gérées par la solution MDM (Mobile Device Management). En cas de perte ou de vol, les données stockées sur les appareils mobiles peuvent être effacées à distance par CACEIS.

6.5.5 Élimination des PC et supports de données usagés

CACEIS a défini et mis en œuvre des procédures appropriées (SOP) pour le transport et l'élimination sécurisés des actifs TIC, les supports de stockage de données étant soumis à la norme de destruction EN 66399. CACEIS a également défini et mis en œuvre des procédures appropriées (SOP) pour l'effacement sécurisé des données du stockage. médias.

6.6 Contrôle de disponibilité

6.6.1 Installations de sécurité dans les zones matérielles (salles de serveurs, centre de données)

Les systèmes d'information sont hébergés dans des centres de données de niveau IV qui répondent aux exigences de protection et de sécurité les plus élevées. Les centres de données de niveau IV sont protégés contre les coupures de courant et les pertes de courant et ils sont tous deux situés dans des zones qui ne sont pas soumises aux inondations ni à l'activité sismique. Pour répondre à des critères exigeants, l'électricité et les télécommunications sont sécurisées via de nombreuses entrées.

6.6.2 Sauvegarde de données

La gestion de la sauvegarde et de la récupération des données s'effectue comme suit :

- Des SOP ont été développées pour garantir la sauvegarde et la restauration des systèmes conformément aux exigences métier prédéfinies.
- Les sauvegardes sont effectuées quotidiennement et mises en miroir sur le site secondaire.
- Les procédures de sauvegarde et de récupération sont testées au moins une fois par an pour garantir qu'elles sont pleinement opérationnelles et maintenues à jour.

6.6.3 Précautions contre les catastrophes

CACEIS accompagne un certain nombre de scénarios de crise majeurs prédéfinis du Crédit Agricole et a mis en place des SOP pour y répondre en cas de sinistre.

Quant à nos datacenters, ils sont insensibles aux pannes, capables de résorber de manière autonome une panne de ses datacenters partenaires et d'assurer la continuité de la prestation de services. Nos plans de gestion de crise assurent une gestion du basculement.

CACEIS réalise plusieurs tests par an pour s'assurer que les mesures techniques et organisationnelles en cas de sinistre sont opérationnelles. Ces tests sont réalisés sous le contrôle de la ligne métier qui valide le résultat des tests.

6.7 Piste d'audit pour la saisie, les modifications et les effacements de données personnelles

L'accès aux données (saisies, modifications, effacements) à l'aide des applications d'entreprise est enregistré par les applications elles-mêmes, les applications disposent d'une solution de surveillance réalisée par l'entreprise.

Les utilisateurs individuels accédant aux données personnelles sont également enregistrés et surveillés. Cela signifie que les accès aux données personnelles stockées dans les applications sont surveillés et enregistrés (lecture, écriture, mise à jour, ..).

Les activités d'administration (par exemple, enregistrement des tentatives de connexion, des exceptions, des erreurs, etc.) sont entièrement enregistrées et les journaux d'événements sont régulièrement examinés. Des actions dédiées sont mises en œuvre lorsque cela est approprié pour atténuer tout risque lié au processus. Le contrôle prend le résultat de la surveillance et effectue des actions correctives pour remédier à toute violation spécifique des règles de l'entreprise. CACEIS IT Security Officer est chargé d'initier la démarche dédiée.

Pour le contrôle des données non structurées, CACEIS s'appuie sur la solution Varonis pour contrôler les droits d'accès aux annuaires partagés et l'accès à ces données.

6.8 Suppression des données et limitation du traitement

La politique de conservation des données de CACEIS consiste à ne conserver les données que pendant la durée légale, réglementaire ou contractuelle.

6.9 Contrôle de la sous-traitance

Les prestations correspondant à des critères prédéfinis font l'objet d'un suivi attentif selon les Référentiels prédéfinis du Crédit Agricole pour les Services Essentiels Externalisés (OES) (PSEE). Celles-ci sont complétées par une politique d'externalisation informatique spécifique de CACEIS basée sur la norme ISO 37500. Tous les sous-traitants sont soumis aux clauses de confidentialité de CACEIS et à la Politique de Sécurité des Informations de CACEIS.

Tous les sous-traitants sont évalués annuellement sur la base d'un questionnaire de conformité ou, dans certains cas, par des audits.