Note sur l'impact de la réglementation FIDA sur nos métiers

règlement du Parlement européen et du Conseil relatif à un cadre pour l'accès aux données financières et modifiant les règlements (UE) n°1093/2010, (UE) n° 1094/2010, (UE) n° 1095/2010 et (UE) 2022/2554:

La proposition de la Commission européenne pour un nouveau cadre d'accès aux données financières (aussi dénommée FIDA) a pour objectif de permettre aux consommateurs et aux entreprises d'autoriser des tiers (les utilisateurs de données) à accéder à leurs données détenues par des institutions financières (les détenteurs de données). Les utilisateurs de données pourront alors, sur la base de ces données, proposer des produits et services personnalisés.

Sont concernés :

L'article 2 du règlement FIDA définit à quelle donnée client va s'appliquer le règlement et quelles sont les entités concernées par celui-ci :

Les données concernées par le règlement FIDA :

- les données relatives aux contrats de crédit hypothécaire, aux prêts et aux comptes, à l'exception des comptes de paiement au sens de la directive (UE) 2015/2366 sur les services de paiement, y compris les données sur les conditions, les soldes et les transactions ;
- les données relatives à l'épargne et aux investissements dans des instruments financiers, des produits d'investissement fondés sur l'assurance, des crypto-actifs, des biens immobiliers et d'autres actifs financiers liés, ainsi qu'aux avantages économiques tirés de ces actifs, y compris les données collectées aux fins de la réalisation d'une évaluation de l'adéquation et du caractère approprié conformément à l'article 25 de la directive 2014/65/UE du Parlement européen et du Conseil ;
- les données relatives aux droits à pension dans le cadre de régimes de retraite professionnelle ;
- les données relatives aux produits d'assurance non-vie conformément à la directive 2009/138/CE, à l'exception des produits d'assurance maladie et santé, y compris les données collectées aux fins d'apprécier les exigences et les besoins du client et les données collectées aux fins d'une évaluation de l'adéquation et du caractère approprié ;
- les données relevant d'une évaluation de la solvabilité d'une entreprise qui sont collectées dans le cadre d'une procédure de demande de prêt ou d'une demande de notation de crédit.

Les entités concernées par le règlement FIDA sont :

- les établissements de crédit ;
- les établissements de paiement, y compris les prestataires de services d'information sur les comptes et les établissements de paiement exemptés en vertu de la directive (UE) 2015/2366;
- les établissements de monnaie électronique, y compris les établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE du Parlement européen et du Conseil ;

- **les entreprises d'investissement au sens de la directive MIF 2**;
- les prestataires de services sur cryptoactifs ;
- les émetteurs de jetons se référant à un ou des actifs ;
- les gestionnaires de fonds d'investissement alternatifs ;
- les sociétés de gestion d'organismes de placement collectif en valeurs mobilières;
- les entreprises d'assurance et de réassurance ;
- **les intermédiaires d'assurance et les intermédiaires d'assurance à titre accessoire ;**
- les institutions de retraite professionnelle ;
- les agences de notation de crédit ;
- les prestataires de services de financement participatif ;
- les fournisseurs de PEPP ;
- les prestataires de services d'information sur les comptes ;

Ce règlement ne s'applique pas aux intermédiaires d'assurance, intermédiaires de réassurance et intermédiaires d'assurance à titre accessoire qui sont des microentreprises ou des petites ou moyennes entreprises en vertus de l'article 2, paragraphe 3, points a) à e), du règlement (UE) 2022/2554.

Les microentreprises et PME sont définies dans le décret d'application de la loi de modernisation de l'économie (décret n° 2008-1354) de la manière suivante :

- Microentreprise : elle emploie moins de 10 personnes et son chiffre d'affaires annuel (montant d'argent perçu à une période donnée) ou son bilan (état des actifs et des passifs de la société) n'excède pas 2 millions d'euros ;
- Petite entreprise : elle emploie moins de 50 personnes et son chiffre d'affaires ou son bilan n'excède pas 10 millions d'euros ;
- Moyenne entreprise : elle emploie moins de 250 personnes et son chiffre d'affaires n'excède pas 50 millions d'euros ou son bilan n'excède pas 43 millions d'euros.

Le règlement FIDA définit 3 parties :

- Le client ;
- Le détenteur des données ;
- L'utilisateur des données.

Il faut préciser qu'une entité peut être à la fois détenteur et utilisateur des données.

Le détenteur des données

C'est un établissement financier, autre qu'un prestataire de services d'information sur les comptes, qui collecte, conserve et traite d'une autre manière les données visées à l'article 2, paragraphe 1 ;

Le détenteur des données doit, à la demande de son client par voie électronique, mettre à la disposition d'un utilisateur de données, les données de ce client, il n'en reste pas moins que ce partage de données ne sera fait que dans les conditions et pour les raisons indiquées par le client.

Lorsque le détenteur des données transfère des données à un utilisateur à la demande d'un client, il doit :

- mettre les données client à la disposition de l'utilisateur de données dans un format fondé sur des normes généralement admises et au moins de la même qualité que celle dont il bénéficie ;
- communiquer de manière sécurisée avec l'utilisateur de données en garantissant un niveau de sécurité approprié pour le traitement et la transmission des données client ;
- demander à l'utilisateur de données de démontrer qu'il a obtenu du client la permission d'accéder aux données client de ce dernier que lui-même détient ;
- fournir au client un tableau de bord des permissions, pour le suivi et la gestion des permissions conformément à l'article 8 ;
- respecter la confidentialité des secrets d'affaires et les droits de propriété intellectuelle dans le cadre de tout accès aux données client conformément à l'article 5, paragraphe 1.

L'utilisateur des données

C'est une entité visée à l'article 2, paragraphe 2, qui, après avoir reçu la permission d'un client, dispose d'un accès licite à ses données, telles que visées à l'article 2, paragraphe 1.

L'utilisateur des données pour pouvoir avoir accès aux données détenues par un détenteur doit avoir obtenu l'agrément **d'établissement de crédit, ou de prestataire de services d'information financière conformément à l'article 14,** faute de quoi il ne pourra pas avoir accès aux données client d'un émetteur des données.

L'utilisateur des données doit :

- ne traiter aucune donnée client à des fins autres que la prestation du service explicitement demandée par le client ;
- respecter la confidentialité des secrets d'affaires et les droits de propriété intellectuelle dans le cadre de tout accès aux données client, conformément à l'article 5, paragraphe 1 ;
- prendre des mesures techniques, juridiques et organisationnelles appropriées afin d'empêcher le transfert de données à caractère non-personnel ou l'accès à celles-ci dans les cas où ceux-ci sont illicites au regard du droit de l'Union ou du droit national d'un État membre ;
- prendre les mesures nécessaires pour garantir un niveau de sécurité approprié pour la conservation, le traitement et la transmission des données client à caractère non-personnel;
- ne pas traiter les données client à des fins publicitaires, sauf à des fins de prospection conformément au droit de l'Union et au droit national ;
- s'il fait partie d'un groupe d'entreprises, l'accès aux données client visées à l'article 2, paragraphe 1, et leur traitement, ne sont effectués que par l'entité du groupe qui agit en tant qu'utilisateur de données.

L'utilisateur des données doit effacer les données du client qu'il a reçues par le biais de l'émetteur à partir du moment où l'objectif donné par le client pour lequel le transfert de données a eu lieu est rempli.

Dans les 18 mois suivant l'entrée en vigueur du règlement FIDA, les détenteurs de données et les utilisateurs de données devront s'affilier à un système de partage des données financières régissant l'accès aux données client conformément à l'article 10.

Le prestataire de services d'information financière

Le règlement FIDA introduit un nouvel agrément pour pouvoir être utilisateur des données, ce nouvel acteur est « prestataire de services d'information financière ». Pour ce faire, ce nouvel acteur devra être agréé par l'autorité compétente d'un état membre (AMF, ACPR).

Pour obtenir l'agrément, il faudra fournir les pièces suivantes (article 12) :

a) un programme d'activité indiquant, en particulier, le type d'accès aux données envisagé ;
b) un plan d'affaires contenant notamment un budget prévisionnel afférent aux trois premiers exercices, qui démontre que le demandeur est en mesure de mettre en œuvre les systèmes, ressources et procédures appropriés et proportionnés nécessaires à son bon fonctionnement ;
c) une description du dispositif de gouvernance d'entreprise et des mécanismes de contrôle interne du demandeur, notamment de ses procédures administratives, de gestion des risques et comptables, ainsi que de ses dispositions relatives à l'utilisation de services TIC au sens du règlement (UE) 2022/2554 du Parlement européen et du Conseil, qui démontre que ce dispositif de gouvernance, ces mécanismes de contrôle interne et ces procédures sont proportionnés, adaptés, sains et adéquats ;
d) une description de la procédure mise en place pour assurer la surveillance, le traitement et le suivi des incidents de sécurité et des réclamations de clients liées à la sécurité, y compris un mécanisme de signalement des incidents qui tient compte des obligations de notification fixées au chapitre III du règlement (UE) 2022/2554 ;
e) une description des dispositions en matière de continuité des activités, y compris une désignation claire des opérations critiques, une politique et des plans de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC efficaces, ainsi qu'une procédure prévoyant de tester et de réexaminer régulièrement le caractère adéquat et l'efficacité de ces plans conformément au règlement (UE) 2022/2554 ;
f) un document relatif à la politique de sécurité, comprenant une analyse détaillée des risques liés aux activités du demandeur et une description des mesures de maîtrise et d'atténuation prises pour protéger ses clients de façon adéquate contre les risques décelés en matière de sécurité, y compris la fraude ;
g) une description de l'organisation structurelle du demandeur, ainsi qu'une description de ses accords d'externalisation ;
h) l'identité des dirigeants et des personnes responsables de la gestion du demandeur et, s'il y a lieu, des personnes responsables de la gestion de ses activités d'accès aux données, et la preuve de ce qu'ils jouissent de l'honorabilité et possèdent les compétences et l'expérience requises pour accéder aux données conformément au présent règlement ;
i) le statut juridique et les statuts du demandeur ;
j) l'adresse de l'administration centrale du demandeur ;

k) le cas échéant, l'accord écrit conclu entre le prestataire de services d'information financière et son représentant légal, attestant la désignation de ce dernier, l'étendue de sa responsabilité et les tâches qu'il doit accomplir conformément à l'article 13.

Aux fins du premier alinéa, points c), d) et g), le demandeur fournit une description des dispositions qu'il a prises en matière d'audit et des dispositions organisationnelles qu'il a arrêtées en vue de prendre toute mesure raisonnable pour protéger les intérêts de ses clients et garantir la continuité et la fiabilité de ses activités.

La description des mesures de maîtrise et d'atténuation des risques en matière de sécurité prévue au premier alinéa, point f), indique comment le demandeur garantira un niveau élevé de résilience opérationnel numérique conformément au chapitre II du règlement (UE) 2022/2554, en particulier en ce qui concerne la sécurité technique et la protection des données, y compris pour les systèmes logiciels et de TIC qu'il utilise ou qu'utilisent les entreprises auxquelles il externalise tout ou partie de ses activités.

De plus, il devra aussi avoir une assurance de responsabilité civile professionnelle couvrant les territoires où ils ont accès à des données, ou une autre garantie comparable, et veillent :

a) à pouvoir assumer leur responsabilité en cas d'accès non autorisé ou frauduleux à des données ou d'utilisation non autorisée ou frauduleuse de données ;
b) à pouvoir couvrir la valeur de tout dépassement de la franchise ou autre seuil de l'assurance ou de la garantie comparable ;
c) à assurer un suivi continu de la couverture offerte par l'assurance ou la garantie comparable.

À titre d'alternative à la possession d'une assurance de responsabilité civile professionnelle ou d'une autre garantie comparable telle que requise au premier alinéa, l'entreprise visée au précédent alinéa doit détenir un capital initial de 50 000 EUR, pouvant être remplacé par une assurance de responsabilité civile professionnelle ou une autre garantie comparable dans les meilleurs délais après le début de son activité de prestataire de services d'information financière.

Pour pouvoir utiliser les données d'un émetteur qui se trouve dans un état membre différent, le prestataire de services d'information doit désigner par écrit une personne morale ou physique comme leur représentant légal dans l'un des États membres à partir duquel ils entendent accéder aux données financières.(article 13)

Le prestataire de services d'information financière doit répondre aux exigences suivantes :

a) il met en place des politiques et des procédures suffisantes pour garantir le respect, y compris par ses dirigeants et ses salariés, de ses obligations au titre du présent règlement ;
b) il prend des mesures raisonnables pour assurer la continuité et la régularité de ses activités. À cette fin, le prestataire de services d'information financière utilise des systèmes, des ressources et des procédures appropriés et proportionnés pour assurer la continuité de ses opérations critiques, et il met en place des plans d'urgence et une procédure pour tester et réexaminer régulièrement l'adéquation et l'efficacité de ces plans ;

c) s'il confie à un tiers des fonctions critiques pour la fourniture aux clients d'un service continu et satisfaisant et pour l'exercice d'activités de manière continue et satisfaisante, il prend des mesures raisonnables pour éviter tout risque opérationnel supplémentaire injustifié. L'externalisation de fonctions opérationnelles importantes ne peut être faite d'une manière qui nuise sensiblement à la qualité du contrôle interne du prestataire de services d'information financière et qui empêche l'autorité de surveillance de contrôler qu'il respecte toutes ses obligations ;
d) il dispose de procédures administratives, comptables, de gouvernance saine, de mécanismes de contrôle interne, de procédures d'évaluation et de gestion des risques efficaces et de dispositifs efficaces de contrôle et de sauvegarde de ses systèmes de traitement de l'information ;
e) ses dirigeants et les personnes responsables de sa gestion, ainsi que les personnes responsables de la gestion de ses activités d'accès aux données, jouissent d'une honorabilité et possèdent les connaissances, les compétences et l'expérience requises, tant individuellement que collectivement, pour exercer leurs missions ;
f) il établit et maintien des procédures efficaces et transparentes pour assurer une surveillance, un traitement et un suivi rapides, impartiaux et cohérents des incidents de sécurité et des réclamations de clients liées à la sécurité , notamment un mécanisme de signalement des incidents qui tienne compte des obligations de notification définies au chapitre III du règlement (UE) 2022/2554.

Sanction pour non-respect du règlement FIDA

Dans l'hypothèse où le présent règlement ne serait pas respecté par les différents acteurs, le règlement prévoit les sanctions suivantes :

a) une déclaration publique précisant l'identité de la personne physique ou morale responsable et la nature de l'infraction ;
b) une injonction ordonnant à la personne physique ou morale responsable de mettre fin au comportement constitutif de l'infraction et de s'abstenir de le réitérer ;
c) la restitution des gains retirés de cette infraction ou des pertes qu'elle a permis d'éviter, dans la mesure où il est possible de les déterminer ;
d) la suspension temporaire de l'agrément d'un prestataire de services d'information financière;
e) une amende administrative maximale d'au moins deux fois le montant des gains retirés de l'infraction ou des pertes qu'elle a permis d'éviter, s'il est possible de les déterminer, même si cette amende dépasse les montants maximaux indiqués au point f) du présent paragraphe, pour les personnes physiques, ou au paragraphe 4, pour les personnes morales ;
f) **dans le cas d'une personne physique, une amende administrative maximale, allant jusqu'à 25 000 EUR par infraction et jusqu'à un total de 250 000 EUR par an** ou, dans les États membres dont la monnaie officielle n'est pas l'euro, la valeur correspondante dans la monnaie officielle de l'État membre concerné au... [OP: prière d'insérer la date d'entrée en vigueur du présent règlement] ;
g) l'interdiction temporaire, pour tout membre de l'organe de direction du prestataire de services d'information financière, ou pour toute autre personne physique, qui sont tenus pour responsable de l'infraction, d'exercer des fonctions de direction au sein d'un prestataire de services d'information financière ;

h) en cas d'infraction répétée aux articles mentionnés au paragraphe 1, l'interdiction pendant au moins dix ans, pour tout membre de l'organe de direction du prestataire de services d'information financière, ou pour toute autre personne physique, qui sont tenus pour responsable de l'infraction, d'exercer des fonctions de direction au sein d'un prestataire de services d'information financière.

Les États membres veillent, conformément à leur droit national, à ce que les autorités compétentes aient le pouvoir d'imposer, pour la commission par **des personnes morales** des infractions visées au paragraphe 1, des amendes administratives maximales :

a) allant jusqu'à **50 000 EUR par infraction et jusqu'à un total de 500 000 EUR par an** ou, dans les États membres dont la monnaie officielle n'est pas l'euro, la valeur correspondante dans la monnaie officielle de l'État membre concerné au ... [OP: prière d'insérer la date d'entrée en vigueur du présent règlement];
b) **2 % du chiffre d'affaires annuel total de la personne morale** tel qu'il ressort des derniers états financiers disponibles approuvés par l'organe de direction.

Si la personne morale visée au premier alinéa est une entreprise mère ou une filiale d'une entreprise mère qui est tenue d'établir des états financiers consolidés conformément à l'article 22 de la directive 2013/34/UE du Parlement européen et du Conseil , le chiffre d'affaires annuel total à prendre en considération est le chiffre d'affaires net ou les recettes à déterminer, conformément aux normes comptables applicables, d'après les états financiers consolidés de l'entreprise mère ultime disponibles pour la dernière date de clôture du bilan, dont sont responsables les membres des organes d'administration, de direction et de surveillance de cette entreprise mère ultime.

Les États membres peuvent habiliter les autorités compétentes à imposer d'autres types de sanctions administratives et autres mesures administratives, outre celles visées aux paragraphes 3 et 4, et ils peuvent prévoir des montants de sanctions pécuniaires administratives plus élevés que ceux prévus aux dits paragraphes.

Les États membres notifient à la Commission le niveau de ces sanctions plus élevées, ainsi que toute modification ultérieure de ces dernières.

En cas de non-respect des décisions d'une autorité de contrôle, les amendes seront majorées comme suit :

- **3 % du chiffre d'affaires quotidien moyen, dans le cas d'une personne morale;**
- **30 000 EUR, dans le cas d'une personne physique**.

Ces astreintes sont un montant quotidien à payer jusqu'au rétablissement de la conformité et ne pouvant excéder une durée de 6 mois.