Les rendez vous de la regulation

Marie-Agnès Nicolet
Regulation Partners
Présidente fondatrice
30, rue La Boétie - 75008 Paris
Mariagnes.nicolet@regulationpartners.com

Mercredi 11 décembre 2024

Au Programme

I. Le Règlement européen sur l'intelligence artificielle (IA)

II. Le Règlement relatif à l'accès aux données financières (FIDA)

III. Le Règlement sur la résilience opérationnelle numérique (DORA)

I. Le Règlement européen sur l'intelligence artificielle (IA Act)

L'IA ACT

L'IA Act

- Publication du projet de règlement le **21 avril 2021**
- Accord politique entre le Conseil et le Parlement européen le **8 décembre 2023**
- Les 27 États membres de l'Union européenne réunis à Bruxelles ont validé l'AI Act le **2 février 2024**
- Le projet de règlement européen est adopté par le parlement européen, par 523 voix pour et 46 contre le **13 mars 2024**
- Entrée en vigueur du règlement le **1er août 2024**

Approche par les risques

- Classification en 3 niveaux de risque : **risque « inacceptables », risque « élevé », risque « modéré ».**

Contrôle des pratiques IA dans l'UE

- Système de gouvernance au niveau des États membre.
- Création d'un *Bureau de l'IA*.

Sanctions fortes

- 35 millions d'euros ou à 7 % du CA pour les violations des applications d'IA interdites.
- 15 millions d'euros ou à 3 % du CA pour les violations des obligations découlant de la législation sur l'IA.
- 7,5 millions d'euros ou à 1 % du CApour la communication d'informations inexactes, incomplètes ou trompeuses.

L'IA ACT

Calendrier d'entrée en vigueur :

2024 :

1. Publication et entrée en vigueur initiale

- **12 juillet 2024** : Publication officielle de la loi sur l'IA au Journal officiel de l'Union européenne, marquant la notification formelle de la nouvelle législation. **Article 113**

- **1er août 2024** : Entrée en vigueur du règlement. À cette date, aucune obligation spécifique n'est encore imposée aux opérateurs ; les exigences commenceront à s'appliquer progressivement selon le calendrier établi. **Article 113**

2. Premières obligations pour les États membres

- **2 novembre 2024 :** Délai pour que les États membres identifient et publient la liste des autorités ou organismes responsables de la protection des droits fondamentaux liés à l'IA, et qu'ils en informent la Commission européenne ainsi que les autres États membres. En France la CNIL serait l'autorité la plus avancée sur le sujet. **Article 77 2°**

L'IA ACT

Calendrier d'entrée en vigueur :

2025 :

3. Application progressive des interdictions

- **2 février 2025 :** Les interdictions concernant certains systèmes d'IA, définies aux chapitres I et II du règlement, commencent à s'appliquer. **Article 113, a) et Considérant 179**

4. Obligations spécifiques pour les fournisseurs et les États membres

- **2 août 2025** : Plusieurs dispositions deviennent applicables selon **l'article 113 b)** , notamment celles relatives aux :
  - organismes notifiés (**chapitre III, section 4**),
  - aux modèles d'IA à usage général (GPAI) (**chapitre V**)
  - à la gouvernance (**chapitre VIII**) ,
  - à la confidentialité (**article 78**)et
  - aux sanctions (**article 99 et 100**).

L'IA ACT

Calendrier d'entrée en vigueur :

2026 :

5. Application du règlement

- **2 aout 2026** : La majorité des dispositions restantes du règlement deviennent applicables, à l'exception de **l'article 6, paragraphe 1** (Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque) . **Article 113 c).**

2027 :

6. Application complète du règlement

- **2 aout 2027** : Les obligations prévues à **l'article 6, paragraphe 1** (Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque)sont applicables. **Article 113 c).**

Définition juridique d'un système d'IA

Définition de l'IA Act , art 3 1°: *"un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels".*

IA à haut risque

Un système d'IA mis sur le marché ou mis en service, qu'il soit ou non indépendant des produits visés aux points a) et b), est considéré comme étant à haut risque lorsque les deux conditions suivantes sont remplies :

a) le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par les actes législatifs d'harmonisation de l'Union énumérés à l'annexe I, ou le système d'IA constitue lui-même un tel produit;

b) le produit dont le composant de sécurité visé au point a) est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit conformément aux actes législatifs d'harmonisation de l'Union énumérés à l'annexe I.

Exemple :

Systèmes d'IA destinés à être utilisés pour **évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit, à l'exception des systèmes d'IA utilisés à des fins de détection de fraudes financières.**

IA interdite

Quelques exemples de pratiques interdites :

- la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes de catégorisation **biométrique qui catégorisent individuellement les personnes physiques sur la base de leurs données biométriques afin d'arriver à des déductions ou des inférences concernant leur race, leurs opinions politiques, leur affiliation à une organisation syndicale, leurs convictions religieuses ou philosophiques, leur vie sexuelle ou leur orientation sexuelle;** cette interdiction ne couvre pas l'étiquetage ou le filtrage d'ensembles de données biométriques acquis légalement, tels que des images, fondés sur des données biométriques ou la catégorisation de données biométriques dans le domaine répressif;

- la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA **qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance;**

- **l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, sauf si et dans la mesure où cette utilisation est strictement nécessaire eu égard à un des objectifs prévus par le règlement.**

Consultation de la CNIL sur le développement des SIA

Contexte :

- **Lancement de la consultation :** La CNIL a ouvert une consultation publique sur l'intelligence artificielle (IA) **en juin 2024**, dans le but de recueillir les retours de différents acteurs de l'IA et du public sur les enjeux de protection des données et les bonnes pratiques à adopter. **Elle s'est terminée le 1er octobre 2024**.

- **Objectif principal** : Concilier le développement technologique de l'IA avec le respect des droits et libertés des individus.

Objectifs généraux :

- **Évaluation des risques :** Identifier les risques que l'IA représente pour les droits des citoyens, en particulier la protection des données personnelles.

- **Développement d'une régulation équilibrée :** Recueillir des avis sur la manière de mettre en place une régulation de l'IA qui soutienne l'innovation tout en garantissant la protection des droits.

- **Transparence et responsabilité :** Promouvoir des pratiques transparentes et responsables, assurant que les systèmes d'IA sont expliqués de manière accessible aux utilisateurs.

Consultation de la CNIL sur le développement des SIA

Objectifs en matière de données personnelles :

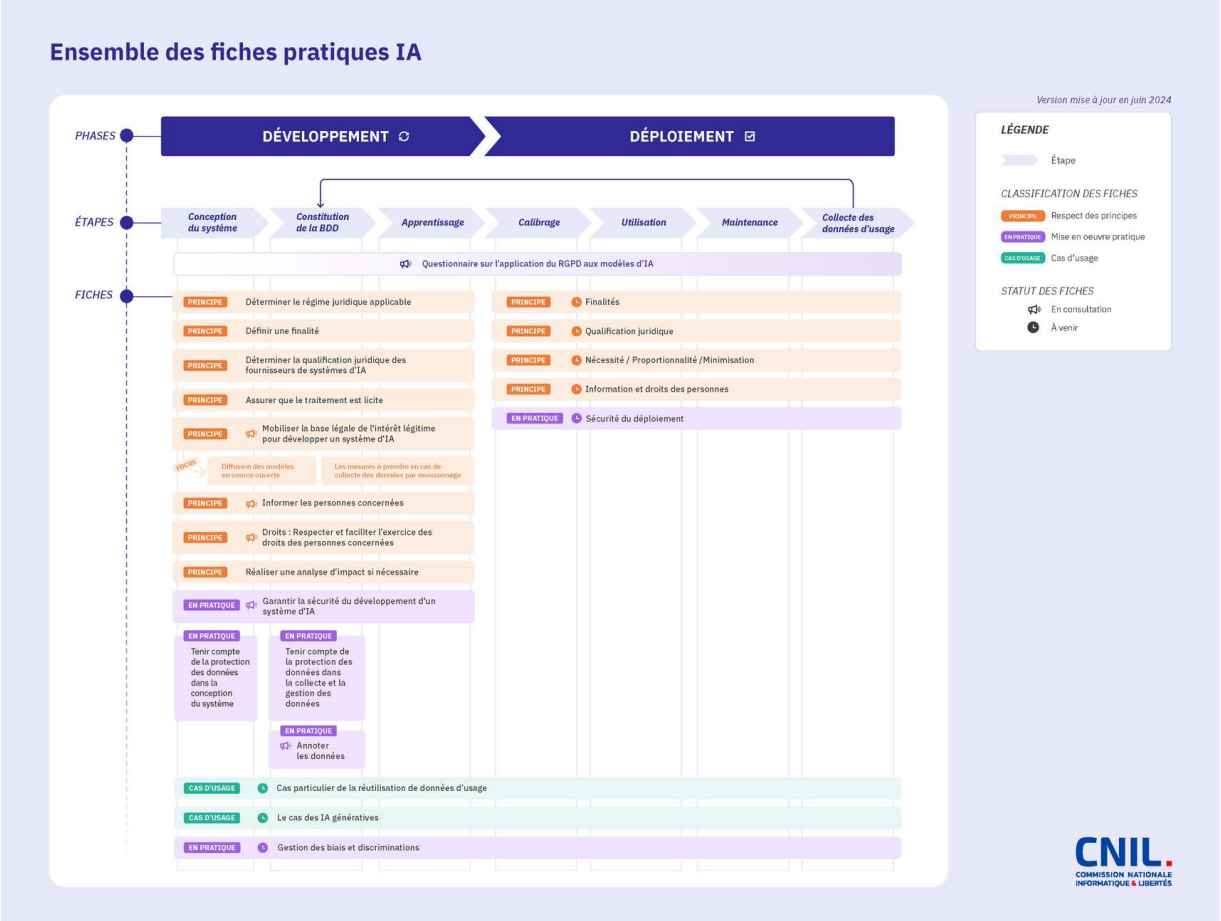
- **Finalité des données** : Garantir que les données personnelles utilisées par l'IA soient collectées et traitées uniquement pour des objectifs précis et légitimes.
- **Minimisation des données** : Réduire au strict nécessaire la collecte de données pour éviter tout traitement excessif.
- **Transparence des algorithmes** : Assurer que les processus de prise de décision automatisés soient compréhensibles et explicables pour les utilisateurs.

Recommandations clés :

- **Conception responsable** : Encourager les entreprises à développer des IA en tenant compte des impacts sociaux, éthiques et environnementaux.
- **Audit des systèmes IA** : Prévoir des mécanismes pour auditer régulièrement les systèmes d'IA afin de vérifier leur conformité avec les règles de protection des données et d'éthique.
- **Amélioration continue** : Mettre en place des procédures de mise à jour et de révision des systèmes d'IA pour intégrer les retours et les évolutions technologiques.

Consultation de la CNIL sur le développement des SIA

Les prochaines étapes ?



Consultation de la commission européennee sur les IA interdites et la définition d’un SIA

Contexte :

- **Lancement de la consultation** : Le 13 novembre 2024, la Commission Européenne a ouvert une consultation publique visant à obtenir des contributions sur la définition des systèmes d'IA et les pratiques interdites dans le cadre de l'AI Act, la première législation européenne sur l'IA. Cette consultation **se clôture le 11 décembre 2024.**

- **Objectif** : Recueillir des avis afin de finaliser les lignes directrices qui clarifieront les interdictions spécifiques et la portée des systèmes d'IA selon la législation en préparation.

Qui peut participer ?

- **Acteurs industriels** :

- **Chercheurs et experts en IA** :

  - **Citoyens et organisations de la société civile** :

Consultation de la commission européennee sur les IA interdites et la définition d’un SIA

Points clés de la consultation :

- **Définition d'un "système d'IA"** : La Commission cherche à préciser quels systèmes peuvent être classifiés comme de l'IA selon les critères technologiques et fonctionnels.

- **Identification des pratiques interdites** : Parmi les interdictions proposées, la Commission se concentre sur des pratiques telles que l'usage abusif des données, la manipulation des comportements humains, ou l'usage d'algorithmes discriminatoires.

- **Réglementation des systèmes à haut risque** : Une attention particulière est portée aux IA utilisées dans des domaines sensibles, comme la santé, la justice ou la sécurité publique.

II. Le Règlement relatif à l'accès aux données financières (FIDA)

Financial Data Access (FIDA)

Réf. du texte : Règlement 2023/0205 (COD)
Thème principal : Finance numérique et données
Périmètre d'application : Union européenne
Acteurs impactés : Le présent règlement s'applique aux entités suivantes lorsqu'elles agissent en tant que **détenteurs de données** ou en tant **qu'utilisateurs de données**. **Article 2 2°.**

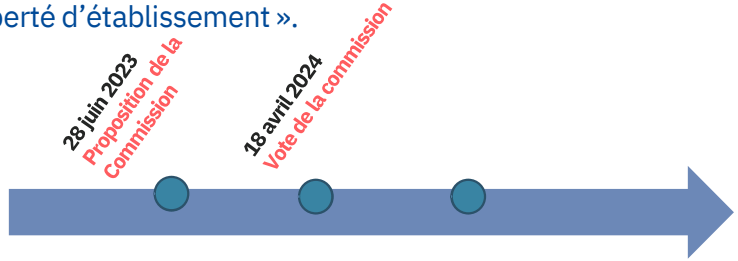
Objectifs

Le règlement FIDA instaure l'obligation pour les **détenteurs de données clients** au-delà des prestataires de services de paiement (les établissements financiers) de **mettre ces données en continu et en temps réel à la disposition des utilisateurs de données** (d'autres établissements financiers régulés ou des prestataires agréés du type Fintech), **lorsque le client en fait la demande dans un objectif précis**.

Impacts

- **Les détenteurs de données** pourront demander une compensation financière raisonnable pour rendre les données accessibles aux utilisateurs de données.
- **Les utilisateurs de données** auront un accès en lecture de ces données, mais ne pourront pas effectuer de transactions pour le compte des clients.
- **Création d'un nouvel agrément** pour les acteurs qui ne sont pas des institutions financières au sens de l'article 28 : « Les prestataires de services d'information financière et les établissements financiers sont autorisés à accéder aux données de clients de l'Union visées à l'article 2, paragraphe 1, qui sont détenues par des détenteurs de données établis dans l'Union, dans le cadre de la libre prestation de services ou de la liberté d'établissement ».

Calendrier



Financial Data Access (FIDA)

Principales définitions à l'article 3 :

- **«données client»** : les données à caractère personnel et non personnel qui sont collectées, conservées et traitées d'une autre manière par un établissement financier dans le cadre de ses relations commerciales normales avec ses clients et qui recouvrent à la fois les données fournies par les clients et les données générées à la suite d'une interaction entre un client et l'établissement financier;

- **«détenteur de données»** : 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; 6) ;

- **«utilisateur de données»** : une entité visée à l'article 2, paragraphe 2, qui, après avoir reçu la permission d'un client, dispose d'un accès licite aux données client de ce dernier, telles que visées à l'article 2, paragraphe 1;

- **«prestataire de services d'information financière»** : un utilisateur de données ayant reçu, en vertu de l'article 14, un agrément lui permettant d'accéder aux données client visées à l'article 2, paragraphe 1, aux fins de la fourniture de services d'information financière.

Financial Data Access (FIDA)

Explications des principales mesures

- **Les actifs concernés** : Le règlement s'applique aux actifs suivants :
  - OPCVM (SICAV et FCP) /
  - FIA (SCPI, FCPI, FIP, FPCI, FCPR, GFI, etc.)
  - Mandat de gestion

- **Ces produits pouvant être détenus en direct ou via** :
  - Un compte-titre
  - Une assurance-vie
  - Un PER
  - Un PEE
  - Un PEPP (Produits paneuropéens d'épargne-retraite individuelle)

- **Les données concernées** :
  - **Seules les données accessibles depuis l'espace client devraient être concernées**
  - Exemple : • Titulaire du compte • Nom et ISIN des fonds • Nombre de parts • Valorisation des parts • Niveau de risque des fonds • Performances des fonds • Mouvements (frais de gestion, versements, retraits, etc.) • Indicateurs ESG des fonds • Profil MIF du client • Etc

Financial Data Access (FIDA)

Impacts pour les acteurs concernés

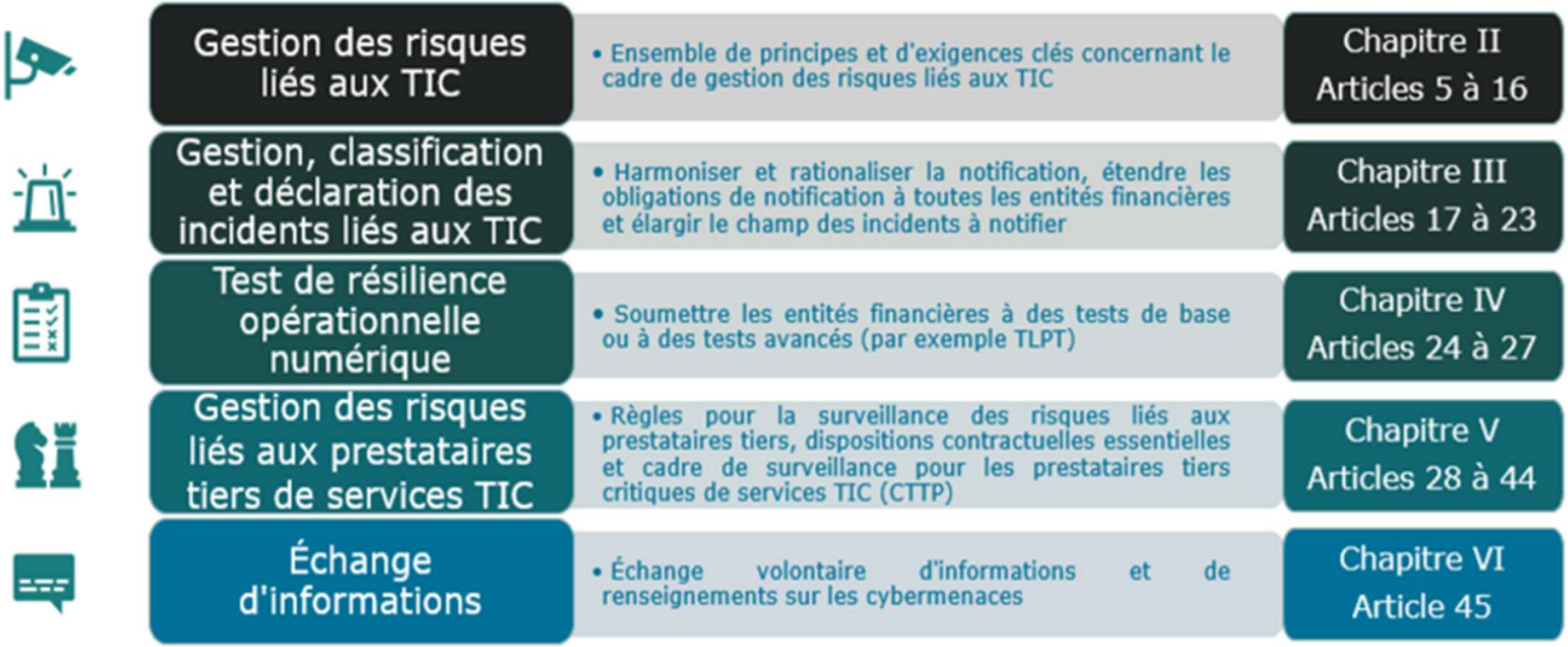
- **Echanges de données** :
  - Les détenteurs de données doivent mettre à disposition des données en temps réel auprès des data users dans un format standardisé (1). Après consentement d'un client (2), la donnée doit être mise à disposition du data user : • dans les meilleurs délais • en temps réel • en continu • gratuitement (ou contre une compensation « raisonnable »). **Article 4**

- **Modalités de gestion du consentement** :
  - Le détenteur de données fournit au client un tableau de bord des permissions pour permettre à celui-ci de suivre et de gérer les permissions qu'il a données à des utilisateurs de données. **Article 8**

- **Compensation financière** :
  - **Article 10 h** *« le système de partage des données financières établit un modèle pour déterminer la compensation maximale qu'un détenteur de données est en droit de facturer pour la mise à disposition de données, via une interface technique appropriée de partage de données avec des utilisateurs de données, conforme aux normes communes. Ce modèle obéit aux principes suivants: i) il limite la compensation à une compensation raisonnable, directement liée à la mise à disposition des données à l'utilisateur de données, et imputable à sa demande; ii) il est fondé sur une méthode objective, transparente et non discriminatoire convenue par les membres; iii) il est fondé sur des données de marché complètes collectées auprès des détenteurs et des utilisateurs de données sur chacun des éléments de coût à prendre en considération, qui est clairement identifié dans le cadre du modèle; iv) il fait l'objet d'un suivi et d'un réexamen réguliers visant à tenir compte des progrès technologiques ».*

III. Le Règlement sur la résilience opérationnelle numérique (DORA)

Les 5 piliers de DORA



Quelques clauses complémentaires dans les contrats de prestations TIC

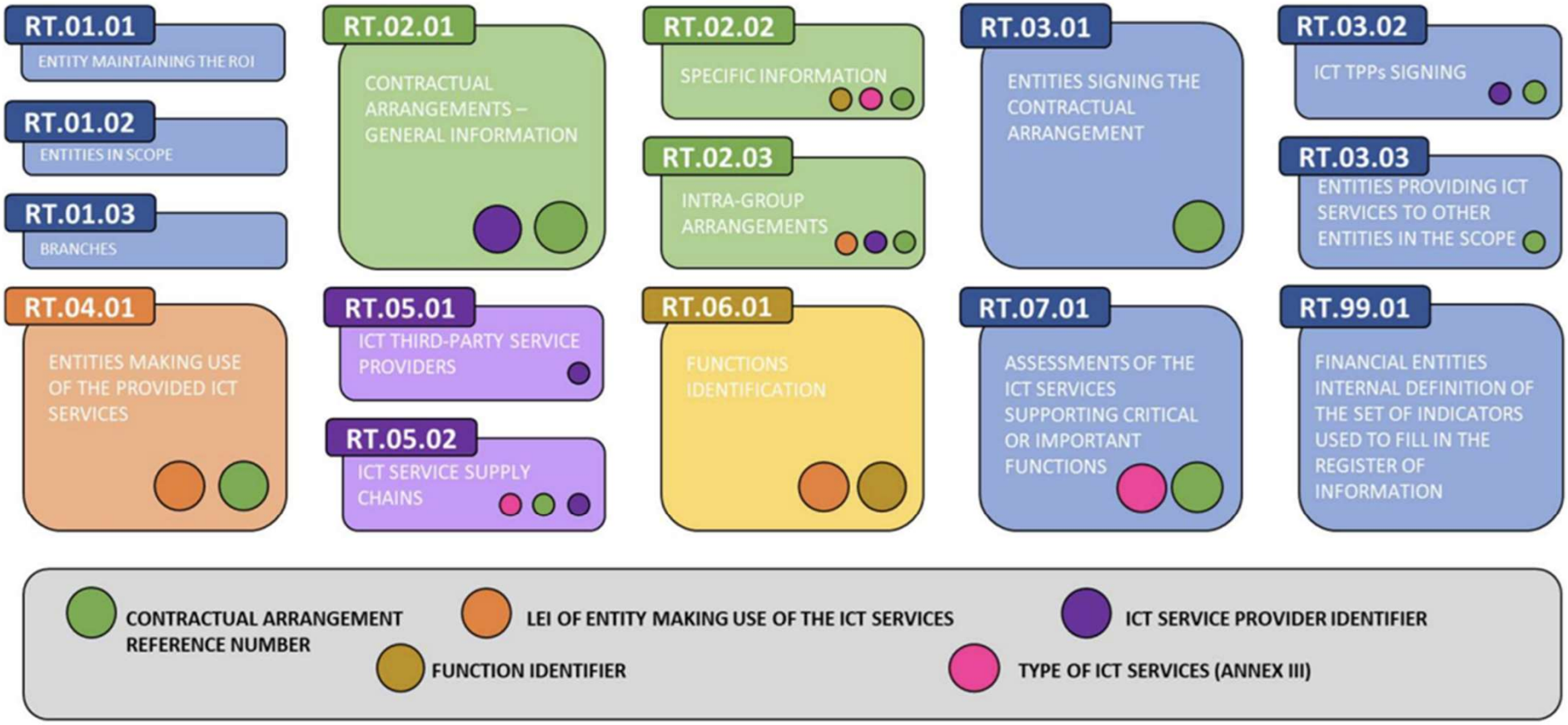
- **Les plans de sortie sont soumis à des tests suffisants et ré-examinés périodiquement**
- **L'obligation pour le prestataire tiers de services TIC de participer et de coopérer pleinement au TLPT**
- **L’obligation de fournir à l’entité financière, sans frais supplémentaires une assistance en cas d’incident TIC**
- **L'obligation de mettre en œuvre et de tester le plan de continuité d’activité**

Quelques différences entre orientations EBA-TIC DORA

Thème	EBA	DORA
Gestion du risque lié aux TIC	**Lignes directrices** sur la gestion des cyber-risques **mais moins détaillées et spécifiques que DORA.**	**Exigences spécifiques pour la gestion des cyber-risques,** y compris l'identification des risques, la protection, la surveillance, la détection et la mise en place de plans de réponse aux des incidents.
Gestion des fournisseurs tiers	**Lignes directrices générales** sur la gestion des risques des fournisseurs tiers, **mais moins prescriptives que DORA.**	**Impose des exigences très strictes** concernant la gestion des risques des fournisseurs tiers critiques, en imposant des règles concernant la résilience, la surveillance continue et la notification des incidents et de continuité d'activité. **Désignation d'un superviseur principal pour chaque fournisseurs tiers (par l'AES)**
Tests de résilience opérationnelle numérique	**Recommande la mise en place de tests réguliers de sécurité et de résilience**, mais ces tests ne sont pas toujours imposés par une législation contraignante.	**Exige des tests obligatoires de résilience,** y compris des tests de continuité des activités et des cyber-risques : **Tests de résilience opérationnelle et de continuité d'activité au moins une fois par an.**

Des différences entre registre PSEE et DORA

Illustration 1: Structure of the Register of Information



Each box represents one template of the Register of information.

RESTONS EN CONTACT

Marie-Agnès Nicolet
Regulation Partners
Présidente fondatrice
30, rue La Boétie - 75008 Paris
marieagnes.nicolet@regulationpartners.com
Tel : +33 6 58 84 77 40