silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

Livre blanc

Codes de conduite RGPD

RÉVISIONS

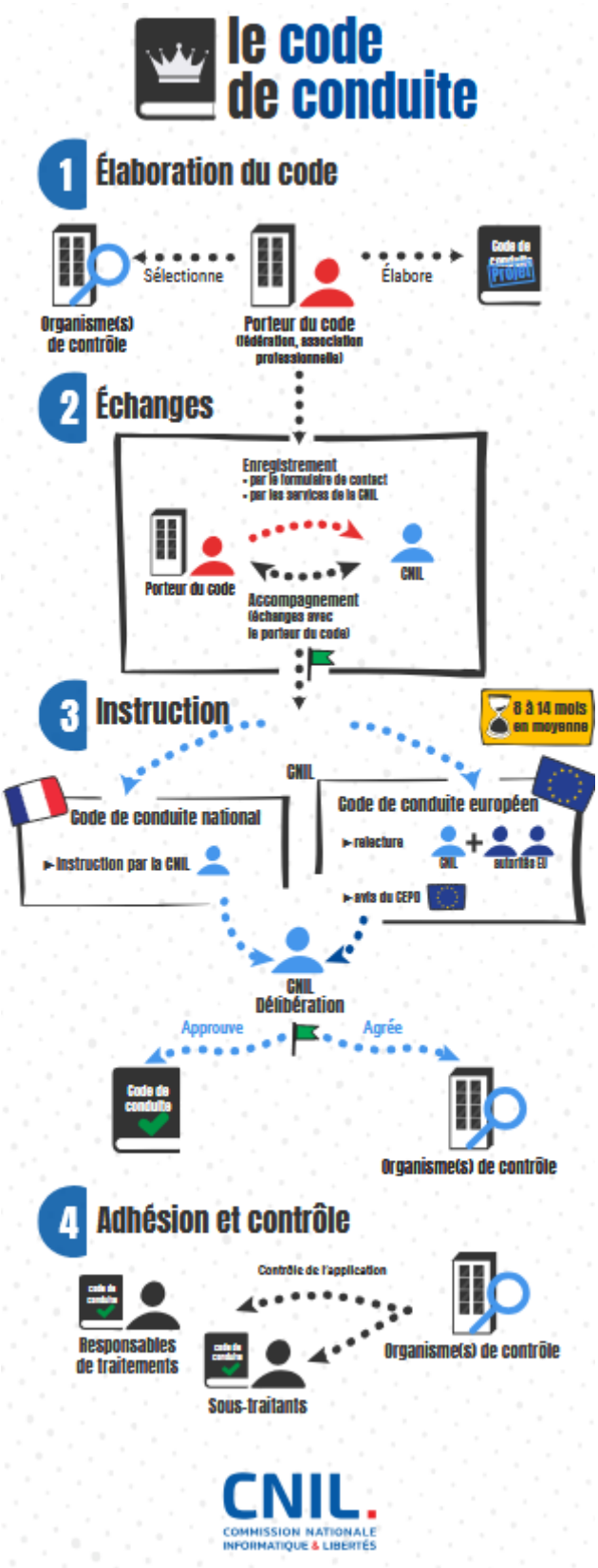
Date	Nature des modifications
14/01/2026	Création du document par la société SILEXO

SOMMAIRE

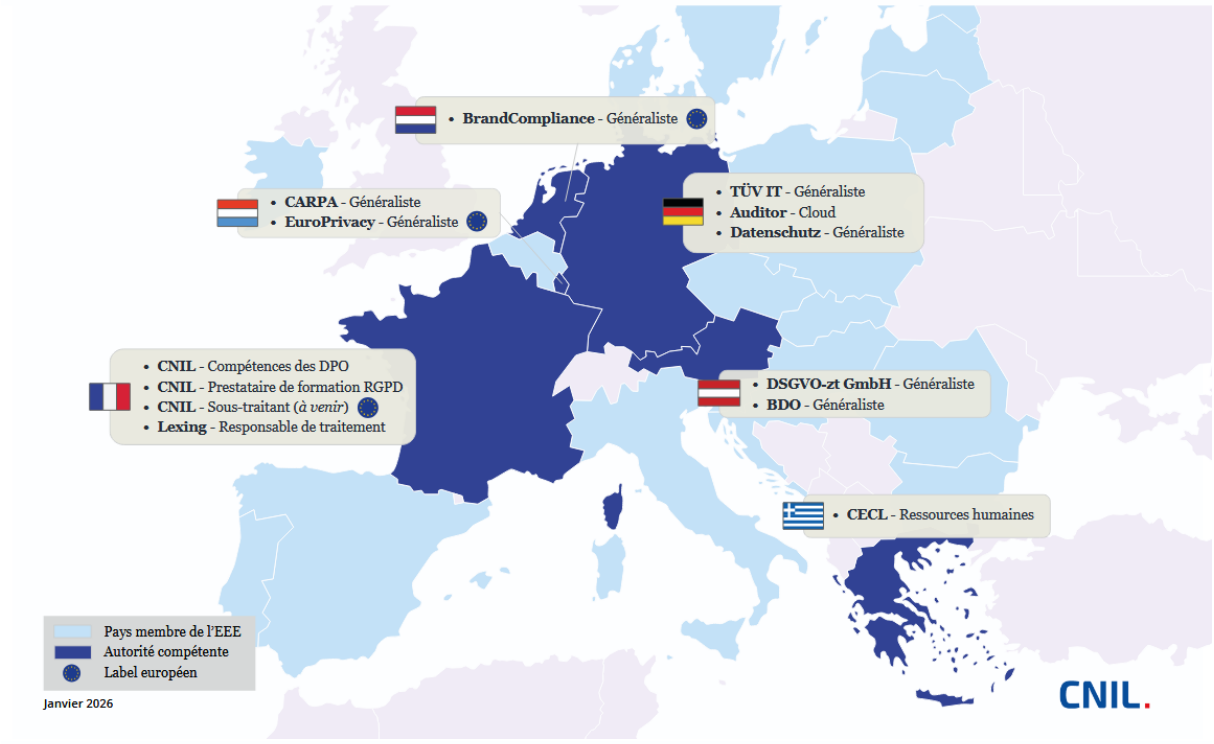
Les certifications et les codes de conduite sont des outils opérationnels facilitant la démarche de mise en conformité des professionnels. Ils permettent d'harmoniser les pratiques au sein d'un secteur d'activité et apportent des garanties appropriées en matière de protection des données.

On en dénombre aujourd'hui une trentaine, tant au niveau national qu'européen : lorsqu'ils sont à portée européenne, ils sont conçus pour être proposés dans toute l'Union européenne.

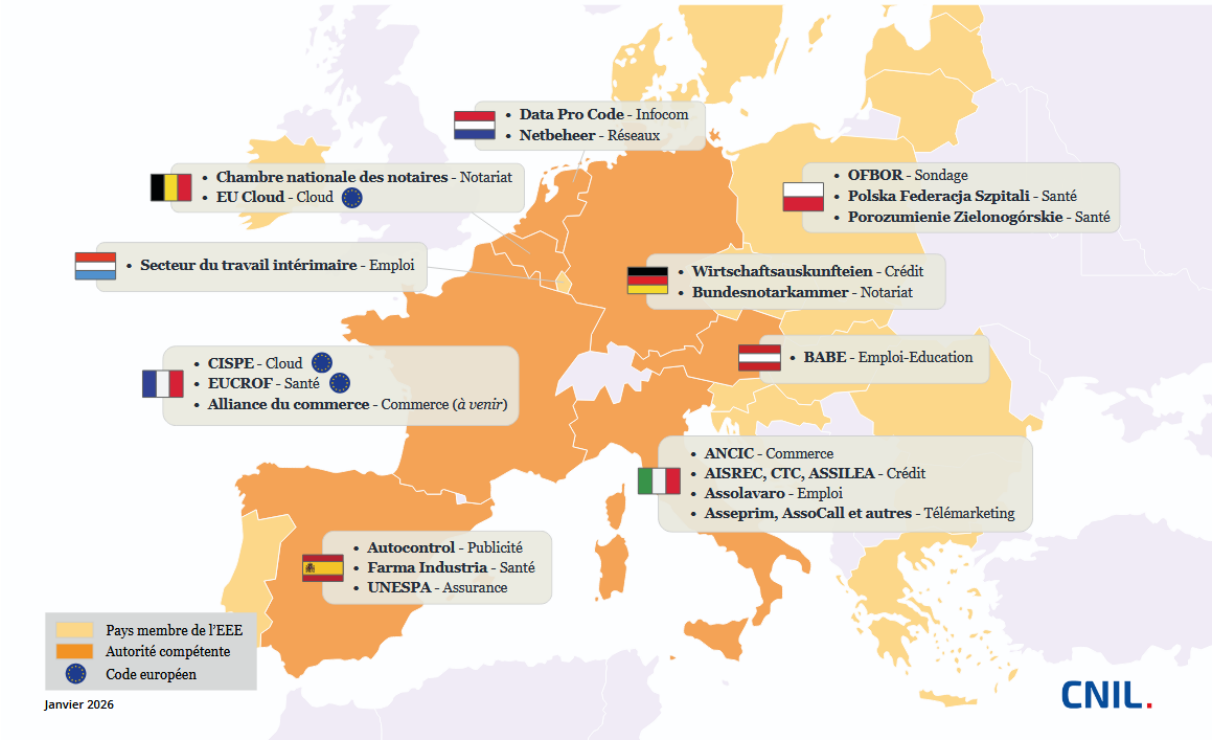
***Note aux lecteurs** : La méthodologie de rédaction de ce livre blanc repose sur une chaîne de traitement outillée par l'IA : ChatGPT a d'abord été utilisé pour concevoir un prompt structurant, servant de cadre d'analyse, puis ce prompt a été injecté dans NotebookLM afin d'interroger directement l'ensemble des codes de conduite, quelles que soient leur langue et leur forme ; cette approche a permis d'extraire, de normaliser et de comparer des contenus juridiques hétérogènes à grande échelle, avant une phase finale strictement humaine de relecture critique, de consolidation juridique et de mise en forme éditoriale, garantissant que le livre blanc repose à la fois sur la puissance de traitement de l'IA et sur une relecture humaine.*


le code de conduite
1 Élaboration du code
Sélectionne
Élabore
Organisme(s) de contrôle
Porteur du code (fédération, association professionnelle)
2 Échanges
Enregistrement
- par le formulaire de contact
- par les services de la CNIL
Porteur du code
CNIL
Accompagnement (échanges avec le porteur du code)
3 Instruction
8 à 14 mois en moyenne
CNIL
Code de conduite national
► instruction par la CNIL
Code de conduite européen
► relecture
CNIL
autorités EU
► avis du CEPD
CNIL Délibération
Approuve
Agrée
Code de conduite
Organisme(s) de contrôle
4 Adhésion et contrôle
Contrôle de l'application
Responsables de traitements
Sous-traitants
Organisme(s) de contrôle
CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Certifications RGPD et Loi informatique et libertés



Codes de conduite RGPD



1 | Tableau de synthèse des codes de conduite

Voici l'inventaire exhaustif des codes de conduite RGPD identifiés dans les sources fournies, structuré selon les critères demandés.

Tableau de synthèse des codes de conduite identifiés

Nom officiel du code	Pays / Autorité	Secteur	Acteurs	Statut	Portée	Contrôle & Sanctions
CISPE Code of Conduct	France / CNIL	Cloud Infrastructure (IaaS)	ST	Reconnu UE	EEE	MB (EY Certifypoint) ; Avertissement, retrait, suspension
EU Cloud Code of Conduct	Belgique / APD	Services Cloud (B2B)	ST	Reconnu UE	EEE	MB ; Blâme, révocation de conformité ou d'adhésion
Data Pro Code	Pays-Bas / AP	Secteur ICT (TPE/PME)	ST	National	Pays-Bas	MB (Data Pro Toezichthouder) ; Retrait du registre
Code Farmaindustria	Espagne / AEPD	Recherche clinique et pharmacovigilance	Mixte (RT/ST)	National	Espagne	Organe de gouvernement (OGCC) ; Blâme, suspension, exclusion
Code Chambre Nat. des Notaires	Belgique / APD	Notariat (activité publique)	RT	National	Belgique	Chambres des notaires (contrôle qualité) ; Sanctions disciplinaires
Code FSI (Intérim)	Luxembourg / CNPD	Travail intérimaire	RT	National	Luxembourg	MB accrédité ; Suspension ou retrait de l'adhésion
Code SIC (Crédit)	Italie / Garante	Systèmes d'infos crédit (SIC)	Mixte (RT/ST)	National	Italie	MB (OdM) accrédité ; Blâme, suspension, révocation
Code ANCIC (Infos comm.)	Italie / Garante	Informations commerciales	RT	National	Italie	MB (OdM ANCIC) ; Blâme public, suspension, exclusion
Code Assolavoro (APL)	Italie / Garante	Agences pour le travail (APL)	RT	National	Italie	MB (OdM) accrédité ; Rappel formel, suspension, exclusion

Code Telemarketing / Teleselling	Italie / Garante	Marketing téléphonique	Mixte	National	Italie	MB (OdM) accrédité ; Rappels, suspension, exclusion
Slim Netbeheer	Pays-Bas / AP	Énergie (Gestionnaires de réseaux)	RT	National	Pays-Bas	MB accrédité (Monitoring Body) ; Mesures correctives, exclusion
AUTOCONTROL	Espagne / AEPD	Publicité et communication comm.	Mixte	National	Espagne	Jury de la publicité ; Sanctions statutaires, rapport à l'AEPD
Code UNESPA (Assurance)	Espagne / AEPD	Systèmes d'infos assurance (fraude)	RT	National	Espagne	MB (OCCC) accrédité ; Blâme, suspension, exclusion
BABE CoC	Autriche / DSB	Éducation privée / Formation	Mixte	National	Autriche	BABE Datenschutz-Ausschuss ; Exclusion du code
Code DW (Auskunfteien)	Allemagne / LDI NRW	Agences de renseignement comm.	RT	National	Allemagne	MB (TIGGES DCO) ; Rappels, menace d'exclusion, exclusion

Légende : RT = Responsable de Traitement ; ST = Sous-traitant ; MB = Monitoring Body (Organisme de suivi).

2 | Détails analytiques des mécanismes identifiés

Statut et organismes de suivi (Monitoring Body) :

La majorité des codes nationaux (Espagne, Italie, Luxembourg, Allemagne) disposent d'un **Monitoring Body (OdM/MB) accrédité** par leur autorité nationale respective selon l'Art. 41 du RGPD.

Exception notable : Le code des **Notaires belges** est dispensé de Monitoring Body accrédité car les notaires y sont considérés comme des autorités ou organismes publics, le contrôle étant assuré par leurs instances disciplinaires internes.

Les codes **CISPE** et **EU Cloud CoC** se distinguent par leur approbation au niveau européen, permettant une harmonisation à l'échelle de l'EEE pour les fournisseurs de services cloud.

Mécanismes de sanctions et retrait :

Le processus est généralement **graduel** : il commence par un rappel ou avertissement (souvent formel), suivi d'une demande de remédiation sous délai (ex: 30 à 60 jours pour CISPE ou les APL italiennes).

En cas de non-conformité persistante, les mesures prévoient la **suspension de l'adhésion** puis l'**exclusion définitive** du code.

Une sanction spécifique récurrente est la **publication du manquement** ou du retrait sur le site web de l'organisme de contrôle ou du porteur du code, visant à informer le marché et les autorités.

Portée géographique :

La quasi-totalité des codes identifiés sont **nationaux**, limitant leur application stricte au territoire de l'autorité qui les a approuvés (Espagne, Italie, Pays-Bas, Autriche, Luxembourg, Allemagne).

Seuls les codes liés au secteur du **Cloud (CISPE, EU Cloud CoC)** ont une portée explicitement **transnationale (EEE)**.

3 | Fiches synthétiques des principaux codes de conduite

Voici les fiches synthétiques des principaux codes de conduite identifiés, structurées selon les exigences opérationnelles.

CISPE (Infrastructure Cloud - IaaS)

Problème résolu : Manque de clarté sur la séparation des responsabilités entre fournisseur d'infrastructure et client, et incertitude sur la réutilisation des données par le fournisseur.

Traitements ciblés : Stockage et traitement automatisé de données clientes sur infrastructure cloud (IaaS).

Obligations clés : Offrir une option de stockage exclusivement dans l'EEE ; interdiction absolue de "data mining" ou profilage pour les besoins propres du fournisseur.

Bénéfices adhérent : Présomption de "garanties suffisantes" au titre de l'Art. 28 du RGPD, facilitant la réponse aux appels d'offres publics et critiques.

Contraintes : Audit annuel par un organisme de contrôle accrédité (MB) ; coût d'audit à charge de l'adhérent ; obligation de transparence totale sur les sous-traitants.

Cas d'usage : Fournisseur IaaS européen souhaitant héberger des données de santé ou administratives.

EU Cloud CoC (Services Cloud SaaS/PaaS/IaaS)

Problème résolu : Difficulté pour les clients B2B d'évaluer la conformité de services cloud complexes et de leurs chaînes de sous-traitance.

Traitements ciblés : Services cloud où le fournisseur agit comme sous-traitant (SaaS, PaaS, IaaS).

Obligations clés : Transparence sur les juridictions de traitement ; assistance active pour les DPIA des clients ; notification de faille en maximum 36h aux clients.

Bénéfices adhérent : Trois niveaux de conformité (auto-évaluation vers audit complet) ; marque de confiance reconnue au niveau européen.

Contraintes : Reporting périodique obligatoire au Monitoring Body ; frais d'adhésion annuels ; procédures strictes de gestion des plaintes.

Cas d'usage : Éditeur SaaS voulant démontrer sa conformité à l'échelle de l'Union européenne.

Farmaindustria (Recherche clinique - Espagne)

Problème résolu : Insécurité juridique sur les bases légales du traitement de données de santé et sur la réutilisation des données pour des recherches futures.

Traitements ciblés : Données de patients dans le cadre d'essais cliniques et de pharmacovigilance.

Obligations clés : Codification (pseudonymisation) obligatoire via un "tiers de confiance" ; protocoles de notification de pharmacovigilance via les réseaux sociaux.

Bénéfices adhérent : Fixation de la base légale sur l'obligation légale (supprime le besoin de consentement RGPD pour le traitement) ; médiation extrajudiciaire des litiges.

Contraintes : Audits systématiques et aléatoires par un organe indépendant ; tenue d'un registre de traitement spécifique ultra-détaillé.

Cas d'usage : Laboratoire pharmaceutique menant des essais multicentriques en Espagne.

Notariat Belge (Chambre Nationale des Notaires)

Problème résolu : Concilier le secret professionnel notarial et l'accès aux sources de données authentiques de l'État avec le RGPD.

Traitements ciblés : Récolte via registres nationaux et insertion des données dans les actes authentiques.

Obligations clés : Désignation d'un DPO spécialisé obligatoire ; accès traçable via cartes eID/eNot ; politique de sécurité informatique écrite imposée.

Bénéfices adhérent : Harmonisation nationale des mesures de protection ; contrôle intégré aux audits de qualité trisannuels de la profession.

Contraintes : Sanctions disciplinaires en cas de manquement ; audit de qualité contraignant tous les trois ans.

Cas d'usage : Étude notariale gérant des données financières, fiscales et de capacité civile.

FSI (Travail Intérimaire - Luxembourg)

Problème résolu : Flou sur la minimisation des données transmises aux entreprises utilisatrices et sur les durées de conservation des CV.

Traitements ciblés : Inscription des candidats, matching de profils et gestion des missions.

Obligations clés : Conservation limitée à 3 ans après le dernier contact ; interdiction de collecter des données via les profils sociaux privés (Facebook/Instagram).

Bénéfices adhérent : Standardisation évitant les demandes excessives de données par les clients (entreprises utilisatrices).

Contraintes : Audit SI externe obligatoire avant l'adhésion ; procédure d'"opt-out" marketing automatisée exigée.

Cas d'usage : Agence d'intérim cherchant à certifier sa gestion de base de données candidats.

Data Pro Code (ICT - Pays-Bas)

Problème résolu : Manque de ressources des PME du numérique pour démontrer leur conformité en tant que sous-traitants.

Traitements ciblés : Maintenance IT, hébergement et fourniture de services logiciels.

Obligations clés : Rédaction d'un "Data Pro Statement" standardisé ; engagement sur une durée de conservation par défaut de 3 mois post-contrat.

Bénéfices adhérent : Utilisation du certificat "Data Pro" comme levier commercial ; clauses contractuelles types déjà approuvées.

Contraintes : Auto-évaluation annuelle validée par une inspection externe ; inscription au registre public obligatoire.

Cas d'usage : SSII néerlandaise gérant des données sensibles pour des clients locaux.

UNESPA (Assurance - Espagne)

Problème résolu : Nécessité de mutualiser les données de sinistralité pour la tarification et la détection des fraudes sans consentement systématique.

Traitements ciblés : Partage de fichiers sur les sinistres automobiles, vols et incendies.

Obligations clés : Seudonimisation stricte pour les statistiques ; interdiction d'utiliser les données des fichiers communs à des fins marketing.

Bénéfices adhérent : Accès légitimé par la loi aux bases de données sectorielles ; protection contre la fraude organisée.

Contraintes : Signature d'un accord de corresponsabilité ; conservation de 3 ans des preuves d'information des clients.

Cas d'usage : Compagnie d'assurance automobile évaluant le risque d'un nouveau client.

BABE CoC (Éducation privée - Autriche)

Problème résolu : Incertitude sur la gestion des notes et évaluations personnelles dans un cadre de formation professionnelle.

Traitements ciblés : Suivi pédagogique des stagiaires et gestion des formateurs.

Obligations clés : Application stricte du principe "besoin d'en savoir" pour les évaluations ; audits de sécurité physique des locaux de formation.

Bénéfices adhérent : Garantie de fiabilité vis-à-vis du service public de l'emploi (AMS) ; réduction des risques de litiges avec les stagiaires.

Contraintes : Audit externe tous les trois ans ; obligation de formation continue des personnels au RGPD.

Cas d'usage : Prestataire privé autrichien opérant des mesures de réinsertion professionnelle.

4 | Lecture comparative

Cette analyse comparative explore la manière dont les codes de conduite spécialisent le RGPD pour répondre aux besoins métiers, tout en soulignant les orientations stratégiques divergentes selon les autorités et les secteurs.

Ce que les codes standardisent réellement (et les angles morts)

Les codes identifiés apportent une couche de précision opérationnelle que le RGPD laisse volontairement ouverte :

Spécification des mesures techniques et organisationnelles (TOM) : La plupart des codes, comme le **EU Cloud CoC** ou le **CISPE**, traduisent les exigences de l'Article 32 en contrôles auditables précis (souvent indexés sur l'ISO 27001). Ils fixent des standards pour le chiffrement, la gestion des accès et la sécurité physique.

Harmonisation des durées de conservation : C'est un apport majeur des codes sectoriels nationaux. Le code **FSI (Luxembourg)** fixe par exemple à **3 ans** le délai de conservation des données des candidats, tandis que le code **UNESPA (Espagne)** standardise à **5 ans** la conservation des données de sinistres pour la lutte contre le fraude.

Normalisation des relations Responsable de traitement (RT) / Sous-traitant (ST) : Les codes spécialisés dans le Cloud ou l'IT (**Data Pro Code**, **CISPE**) standardisent les clauses contractuelles de l'Article 28, facilitant la preuve des "garanties suffisantes".

Protocoles métiers spécifiques : Le code **Farmaindustria** standardise le recours à un **tiers de confiance** pour le codage des données de santé, tandis que les **Notaires belges** standardisent l'usage de cartes d'identité électroniques pour la traçabilité des accès.

Angles morts identifiés :

Transferts hors EEE : À l'exception de modules spécifiques en cours de développement, la plupart des codes (CISPE, Farmaindustria, EU Cloud CoC) précisent explicitement qu'ils ne constituent pas, à ce stade, un mécanisme de transfert suffisant au titre de l'Art. 46 sans mesures additionnelles.

Activités hors-champ : Les codes centrés sur la sous-traitance excluent généralement les traitements où le prestataire agit comme responsable de traitement (gestion administrative, RH interne).

Conseil juridique : L'adhésion ne remplace ni le respect global du RGPD, ni le recours à un avis juridique spécifique à l'organisation.

Différences de philosophie

On observe trois approches majeures dans la conception de ces codes :

Approche "Compliance by Design"

Cette philosophie se retrouve dans les codes régulant des secteurs à hauts risques ou à forte emprise technique.

Exemples : Le code des **Notaires belges** impose des configurations d'accès spécifiques. Le code **Farmaindustria** rend le processus de codage (pseudonymisation) indissociable de la recherche clinique pour garantir la protection par défaut. Le code **Telemarketing (Italie)** impose des mesures par défaut pour empêcher la clonage des numéros appelants.

Approche "Risk Management"

Ici, le code fournit des méthodologies pour évaluer et mitiger les risques selon le contexte spécifique du traitement.

Exemples : Le code **Slim Netbeheer (Énergie)** impose un modèle de DPIA obligatoire pour chaque "use case" de traitement de données de compteurs. Le code **BABE (Éducation)** propose des matrices de risques quantifiées (impact x probabilité) pour les établissements de formation.

Approche "Marché / Label de confiance"

L'objectif est ici commercial et réputationnel : rassurer le client final et simplifier l'audit.

Exemples : Le **EU Cloud CoC** propose **trois niveaux de conformité** allant de l'auto-évaluation à l'audit tiers complet, permettant une différenciation marketing. Le **Data Pro Code** néerlandais est explicitement conçu comme un outil pour les TPE/PME afin qu'elles puissent démontrer leur fiabilité sans DPO interne.

Secteurs où les codes deviennent un quasi-standard de marché

Dans certains domaines, l'adhésion à un code n'est plus seulement une option, mais une exigence opérationnelle pour rester compétitif :

- **Infrastructure et Services Cloud :** Les codes **CISPE** et **EU Cloud CoC** sont devenus les références pour démontrer le respect des Articles 28 et 32 à l'échelle européenne, facilitant l'accès aux marchés publics.
- **Industrie Pharmaceutique :** En Espagne, le code **Farmaindustria** définit les "règles du jeu" pour l'ensemble des laboratoires associés, stabilisant les pratiques de pharmacovigilance et d'essais cliniques.

- **Renseignement Commercial et Crédit :** En Italie (**SIC**) et en Allemagne (**DW**), ces codes régissent la mutualisation des données de solvabilité, harmonisant les délais de suppression et les droits d'accès pour l'ensemble de la profession.
- **Travail Intérimaire :** Les codes comme celui du **FSI (Luxembourg)** ou d'**Assolavoro (Italie)** stabilisent la relation tripartite complexe (agence, intérimaire, client) et préviennent les demandes excessives de données par les entreprises utilisatrices.

5 | Valeur juridique réelle

L'adhésion à un code de conduite n'offre pas une immunité juridique, mais elle constitue un **puissant levier d'accountability** et un élément de preuve de conformité structurée devant les autorités.

Valeur juridique de l'adhésion : Preuve et présomption

L'adhésion à un code de conduite approuvé au sens du RGPD produit des **effets juridiques gradués**, expressément prévus par le règlement et précisés par la pratique des autorités de contrôle, sans toutefois constituer une exonération de responsabilité ni une présomption automatique de conformité.

- **Élément de démonstration de la conformité**

Conformément à l'article 24 §3 du RGPD, l'adhésion à un code de conduite approuvé peut être utilisée comme un élément permettant au responsable de traitement de démontrer le respect de ses obligations en matière de protection des données. Cette adhésion constitue un facteur probant parmi d'autres et ne dispense pas d'une analyse concrète des traitements mis en œuvre.

- **Élément de démonstration des garanties suffisantes des sous-traitants**

Pour les sous-traitants, l'adhésion à un code de conduite approuvé peut être prise en compte, au titre de l'article 28 §5 du RGPD, comme un élément permettant de démontrer qu'ils présentent des garanties suffisantes en matière de mesures techniques et organisationnelles. Cette adhésion ne crée toutefois aucune présomption légale et ne dispense pas le responsable de traitement de son obligation d'évaluation préalable et continue du sous-traitant.

- **Indice de conformité pris en compte par les autorités de contrôle**

Dans la pratique des autorités de protection des données, l'adhésion à un code de conduite approuvé est susceptible d'être considérée comme un indice de conformité ou de maturité organisationnelle, notamment dans le cadre des contrôles et de l'approche fondée sur le risque. Cette prise en compte relève de la pratique administrative et ne constitue pas une règle juridique autonome.

- **Facteur d'atténuation dans la détermination des sanctions**

En cas de manquement au RGPD, le respect d'un code de conduite approuvé est expressément mentionné à l'article 83 §2 j) comme un critère dont les autorités de contrôle doivent tenir compte pour apprécier le montant des amendes administratives éventuelles.

- **Élément à prendre en compte dans les analyses d'impact (DPIA)**

Conformément à l'article 35 §8 du RGPD, le respect d'un code de conduite approuvé doit être dûment pris en compte lors de la réalisation d'une analyse d'impact relative à la protection des données. Il s'agit d'un élément favorable d'appréciation du cadre de conformité, sans que le code ne puisse, à lui seul, valider ou remplacer l'analyse des risques spécifique au traitement concerné.

Attentes concrètes des autorités envers les adhérents

Les autorités de contrôle (CNIL, APD, AEPD, etc.) attendent une conformité **active et vérifiable**, et non purement déclarative :

- **Soumission à un contrôle indépendant :** L'adhérent doit obligatoirement accepter la surveillance d'un **Organisme de suivi (Monitoring Body)** accrédité, qui effectue des audits périodiques et gère les plaintes.
- **Transparence accrue :** Les organisations doivent rendre leur adhésion publique (registres, sites web) et fournir des informations claires aux personnes concernées sur la manière dont le code est appliqué.
- **Coopération totale :** Les adhérents ont l'obligation de fournir sans délai toutes les informations nécessaires à l'Organisme de suivi pour prouver leur respect du code.
- **Capacité de remédiation :** Les autorités attendent que les adhérents corrigent immédiatement les failles détectées par l'Organisme de suivi, sous peine de suspension ou d'exclusion publique du code.

Limites structurelles et angles morts

Malgré ses avantages, le code de conduite rencontre des limites juridiques majeures :

- **Transferts internationaux (Le "mur" de l'Art. 46) :** À ce jour, la plupart des codes (CISPE, Farmaindustria, EU Cloud CoC) indiquent explicitement qu'ils **ne constituent pas** un mécanisme de transfert suffisant vers les pays tiers sans garanties additionnelles (comme des Clauses Contractuelles Types).
- **Responsabilité finale inaliénable :** L'adhésion n'exonère jamais le responsable de traitement de sa **responsabilité finale** ; il doit toujours effectuer ses propres évaluations pour ses traitements spécifiques.
- **Absence d'attestation de conformité universelle :** L'Autorité de Protection des Données rappelle souvent que l'adhésion n'est pas une "certification de conformité" globale de tous les traitements de l'organisation.

Articulation avec les nouvelles réglementations (NIS2, DORA, IA Act)

Les sources disponibles relatives aux codes de conduite RGPD approuvés abordent encore de manière limitée les textes européens les plus récents (notamment DORA et le règlement sur l'IA). Elles permettent néanmoins d'identifier des **logiques d'articulation convergentes**, tout en laissant subsister des **zones d'absence ou d'incertitude juridique**.

- **Directive NIS 2 : complémentarité fonctionnelle en matière de sécurité et de résilience**

Certains codes de conduite sectoriels, tels que le code CISPE pour les fournisseurs de services cloud, reconnaissent que leurs exigences en matière de sécurité des données, de gestion des incidents et de continuité d'activité s'inscrivent dans une logique complémentaire par rapport aux obligations issues de la directive NIS, désormais remplacée par la directive (UE) 2022/2555 (« NIS 2 »).

Cette articulation repose sur une convergence des objectifs (résilience, prévention et notification des incidents), sans pour autant créer de mécanisme de substitution : le respect d'un code de conduite RGPD ne dispense pas de l'application directe et autonome des obligations NIS 2.

- **Standards de sécurité : alignement technique avec NIS 2 et DORA**

La majorité des codes de conduite RGPD approuvés intègrent ou s'appuient sur des référentiels de sécurité reconnus, tels que les normes ISO/IEC 27001 et apparentées. Cet ancrage facilite, sur le plan technique et organisationnel, l'alignement avec les exigences transversales de sécurité prévues par la directive NIS 2 et par le règlement DORA, en particulier en matière de gouvernance de la sécurité, de gestion des risques et de contrôles internes.

Cet alignement demeure toutefois **technique et méthodologique** : il ne crée ni équivalence juridique, ni reconnaissance automatique de conformité entre régimes.

- **Règlement sur l'intelligence artificielle (AI Act) : absence d'articulation formalisée à ce stade**

À ce jour, les sources relatives aux codes de conduite RGPD approuvés ne contiennent pas d'éléments établissant une articulation explicite ou structurée avec le règlement (UE) 2024/1689 sur l'intelligence artificielle.

En l'absence de dispositions spécifiques ou de lignes directrices des autorités compétentes, aucune interaction normative formelle ne peut être déduite entre les codes de conduite RGPD existants et les mécanismes de conformité prévus par le règlement sur l'IA, notamment pour les systèmes d'IA à haut risque. Cette articulation constitue un **point de vigilance et d'évolution future**, susceptible d'être précisé par la pratique, des codes sectoriels dédiés ou des orientations européennes.

6 | Lecture « business »

L'adhésion à un code de conduite constitue un investissement qui transforme la contrainte réglementaire en un avantage concurrentiel, particulièrement dans les secteurs où la confiance est une variable métier critique.

Profils d'organisations pour lesquels l'adhésion est stratégiquement rentable

L'adhésion est particulièrement rentable pour les profils suivants :

- **Les TPE et PME du secteur numérique (SaaS, IaaS) :** Pour ces entreprises, les codes comme le **Data Pro Code** ou le **CISPE** fournissent des « mains courantes » opérationnelles et des outils (ex: le *Data Pro Statement*) qui remplacent avantageusement l'absence de ressources juridiques internes. L'adhésion permet de démontrer des « garanties suffisantes » au titre de l'Article 28 du RGPD, facilitant ainsi l'accès aux marchés des grands comptes et des administrations publiques.
- **Les sous-traitants (Processors) B2B :** Dans le Cloud, l'adhésion au **EU Cloud CoC** ou au **CISPE** réduit drastiquement les coûts de vente en standardisant les réponses aux questionnaires de conformité des clients.
- **Les organisations de secteurs hautement régulés :** Pour les laboratoires pharmaceutiques (**Farmaindustria**), les notaires ou les agences de crédit (**SIC**), le code réduit l'insécurité juridique liée à l'interprétation de concepts flous (ex: durées de conservation, intérêts légitimes) et offre un mécanisme de médiation qui évite les contentieux coûteux devant les tribunaux ou les autorités de contrôle.
- **Les prestataires travaillant avec le secteur public :** Les codes comme **BABE** (Éducation) ou **Slim Netbeheer** (Énergie) simplifient les relations avec les donneurs d'ordre publics en offrant une preuve de fiabilité déjà validée par l'autorité de protection des données.

Cas où l'adhésion peut être perçue comme principalement cosmétique

L'intérêt est réduit, voire purement communicationnel, dans les configurations suivantes :

- **Le statut de « Candidat » prolongé :** Dans les codes comme le **CISPE**, une organisation peut apparaître au registre comme « Candidate au Code » sur la base d'une auto-évaluation pendant une période limitée (12 mois) avant l'audit obligatoire. Si l'organisation n'achève jamais le processus de vérification par l'organisme de suivi (**Monitoring Body**), l'adhésion reste une promesse non tenue.
- **Les entreprises déjà certifiées ISO/IEC 27001 :** Bien que l'alignement soit utile, la valeur ajoutée sur le plan de la sécurité technique est moindre, car de nombreux codes calibrent leurs exigences sur ces standards internationaux déjà existants.
- **Le niveau 1 de conformité (Auto-évaluation) :** Pour le **EU Cloud CoC**, le premier niveau de conformité repose sur des déclarations internes sans audit tiers systématique, ce qui peut limiter la confiance des clients les plus exigeants par rapport aux niveaux 2 et 3.

Opportunités de marché identifiées

La généralisation de ces codes ouvre trois segments de marché pour les professionnels du conseil et de la cybersécurité :

- **Offres d'accompagnement à la mise en conformité :** Il existe un besoin massif d'aide à la rédaction de politiques internes spécifiques requises par les codes, comme

la documentation du modèle de risque ou le remplissage des **Check-lists de conformité**. L'implémentation du *Privacy by design* est un axe de conseil fort.

- **Audits d'adhésion et de renouvellement :** Chaque code exige l'intervention d'un **Monitoring Body** accrédité ou d'auditeurs qualifiés pour vérifier la conformité initiale et annuelle. Cela crée une demande récurrente pour des prestations d'audit spécialisées, notamment pour les niveaux de conformité supérieurs (Level 2 & 3).
- **Outillage de conformité sectorielle :** Le développement de solutions logicielles intégrant nativement les référentiels de ces codes (ex : matrices de risques **Slim Netbeheer**, registres types **APL**) constitue une opportunité pour les éditeurs de GRC (Governance, Risk and Compliance). Le marché demande des outils permettant un suivi continu de la conformité entre deux cycles d'audit.