

CONFORMITÉ RÉGLEMENTAIRE

En bref

Risques clés :

Le non-respect du Règlement Général sur la Protection des Données (RGPD) expose l'entité à des sanctions financières pouvant être très lourdes – jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial lors d'une violation des principes de traitement des données ou du non-respect des conditions de licéité du traitement (Article 83).

Au-delà des amendes, les entreprises risquent d'importantes atteintes à leur réputation (perte de confiance des clients, déficit d'image, etc.) et engagent leur responsabilité civile, notamment via d'éventuelles actions collectives des personnes concernées.

Une violation grave peut également être la source de perturbation plus ou moins importante de l'activité (ex. indisponibilité du SI après une attaque) et mettre en danger la continuité de l'entreprise.

Points critiques à surveiller :

La **conformité RGPD** doit être démontrée par l'entreprise à tout moment (*accountability*¹). Le commissaire aux comptes (CAC) doit donc rester attentif à :

→ La **gouvernance des données** : nomination d'un DPO/DPD (Data Protection Officer/Délégué à la Protection des Données) si requis, politique interne sur la protection de la vie privée des salariés, sensibilisation du personnel aux bonnes pratiques concernant le traitement des données personnelles.

- La **cartographie des traitements** et des flux de données : existence d'un registre des activités de traitement, identification des données sensibles ou des traitements à grande échelle.
- Le **cadre légal et contractuel** : bases légales des traitements (consentement, intérêt légitime...), information des personnes et gestion de leurs droits (accès, rectification, effacement, etc.), contrats conformes avec les sous-traitants.
- La **sécurité et la gestion des incidents** : mesures de sécurité logiques et physiques pour assurer confidentialité, intégrité et disponibilité des données, dispositifs de détection des incidents et procédures de notification des violations à la CNIL sous 72h si nécessaire (Article 33 et 34).

En résumé, l'auditeur devra vérifier que l'entité a mis en place des processus et des contrôles adaptés pour garantir la protection des données personnelles.

1. L'*accountability* désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Séquence 1

Comprendre la thématique

Contexte et enjeux

Le Règlement Général sur la Protection des Données (RGPD) s'inscrit dans un contexte européen d'harmonisation et de renforcement de la protection des données. Entré en vigueur le 25 mai 2018, il poursuit trois objectifs majeurs :

1. **Renforcer les droits des personnes** : portabilité des données, droit à l'oubli, consentement explicite, information en cas de violation, etc.
2. **Responsabiliser les acteurs traitant les données** : obligation de documentation et de preuve de conformité (accountability), privacy by design², obligation de notification des violations, etc.
3. **Crédibiliser la régulation** : coopération renforcée entre autorités de protection des données, sanctions dissuasives, etc.

Le RGPD s'applique à toute organisation qui collecte ou traite des données personnelles de résidents européens, indépendamment de sa localisation géographique. Une donnée à caractère personnel est définie comme toute information se rapportant à une personne physique identifiée ou identifiable, directement (nom, prénom, etc.) ou indirectement (identifiant en ligne, localisation, etc.).

Le paysage réglementaire s'est depuis 2018 enrichi de nouveaux textes qui viennent compléter le RGPD :

- Le règlement ePrivacy qui renforce la protection des communications électroniques
- Le Digital Services Act (DSA) et le Digital Markets Act (DMA) qui imposent des obligations supplémentaires aux grandes plateformes numériques
- La loi française « Informatique et Libertés » a été modifiée à plusieurs reprises pour s'aligner sur ces évolutions européennes
- Le Privacy Shield a été invalidé par la Cour de Justice de l'Union Européenne (arrêt Schrems II) et remplacé par un nouveau cadre transatlantique de protection des données en 2023

A cette réglementation RGPD s'ajoute l'« IA Act », Règlement européen sur l'Intelligence Artificielle (RIA) dont l'objectif est double : protéger les citoyens (sécurité, droits fondamentaux) sans freiner l'innovation. Le RIA veut créer un climat de confiance (une sorte de ceinture de sécurité juridique) pour encourager le développement d'une IA fiable et éthique. Le RIA est entré en vigueur le 1^{er} août 2024, mais avec une entrée en application progressive, du 2 février 2025 au 31 décembre 2030 selon les thématiques,

Les points clés du RIA, qui s'applique à tous les secteurs économiques sont les suivants :

- **Obligations en matière de gestion des risques** : Le RIA Act impose aux entreprises d'évaluer et de gérer les risques associés à l'utilisation de l'IA, notamment ceux qui touchent à la sécurité des données et à la vie privée.
- **Transparence et traçabilité** : L'IA doit être conçue et utilisée de manière transparente. Cela inclut la nécessité de fournir des explications compréhensibles aux utilisateurs lorsqu'une décision automatisée a un impact significatif sur eux.
- **Conformité croisée avec le RGPD** : En ce qui concerne le traitement des données personnelles, le RIA Act impose aux entreprises de respecter les règles de confidentialité et de sécurité des données définies par le RGPD. Cela inclut la mise en place de mécanismes pour garantir la protection des données dans le cadre des traitements automatisés, en particulier ceux impliquant des algorithmes de machine learning.

2. Intégrer dès la conception les principes de protection des données personnelles (« privacy by design »)

Conséquences pour le commissaire aux comptes

Pour le commissaire aux comptes, l'évaluation de la conformité au RGPD s'inscrit principalement dans le cadre :

- De la **NEP 250** « Prise en compte du risque d'anomalies significatives dans les comptes résultant du non-respect des textes légaux et réglementaires »
- De la **NEP 315** « Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives »

Pour le commissaire aux comptes le RGPD s'inscrit comme un texte de catégorie 3, selon la nomenclature proposée par les normes en vigueur. Cependant, il reste nécessaire d'évaluer les risques que les manquements au RGPD font peser sur l'entité contrôlée :

- 1. Impact sur les comptes** : provisions pour risques et charges (contentieux RGPD), amendes administratives, investissements nécessaires à la mise en conformité
- 2. Risques de continuité d'exploitation** : en cas de sanctions importantes ou d'interdiction de traitement des données critiques pour l'activité
- 3. Information dans l'annexe** : vérification de la pertinence de l'information relative aux risques liés à la protection des données personnelles
- 4. Opportunité de missions de prestations** : le commissaire aux comptes peut proposer des missions complémentaires d'accompagnement à la conformité RGPD

L'évaluation des risques liés à la protection des données personnelles peut s'appuyer sur la matrice suivante :

Facteur de risque	Niveau de criticité	Impacts potentiels
Volume et nature des données traitées	Élevé pour les données sensibles (santé, biométrie, opinions, etc.) et les traitements à grande échelle	Sanctions accrues, nécessité d'analyses d'impact
Exposition internationale	Élevé en cas de transferts hors UE	Complexité juridique, exigences supplémentaires
Niveau de maturité de la gouvernance	Criticité inversement proportionnelle à la maturité	Défaut de contrôle interne, inefficacité des mesures
Sensibilité des activités	Élevée pour les secteurs réglementés (santé, finance, etc.)	Contraintes réglementaires supplémentaires
Antécédents de violation	Élevé en cas d'incidents passés	Surveillance accrue des autorités
Sous-traitance et cloud	Élevé en cas de multiples intervenants ou services cloud	Dilution des responsabilités, perte de maîtrise

S'agissant du RIA, le commissaire aux comptes sera conduit à

- **Évaluer les risques associés à l'IA** : Le commissaire aux comptes devra évaluer la conformité croisée des entreprises à la fois au **RIA Act** et au **RGPD** lorsqu'elles utilisent des systèmes d'IA pour traiter des données personnelles. Cela inclut la vérification de la mise en œuvre des évaluations d'impact sur la protection des données (AIPD) lorsque les technologies d'IA impliquent un risque élevé pour les droits et libertés des personnes concernées.

- **Vérifier les critères de transparence** : Il faudra également vérifier que les systèmes d'IA sont transparents et que les utilisateurs sont informés des décisions automatisées qui peuvent les affecter, conformément aux exigences des deux législations.

Séquence 2

Mission du CAC : objectifs, bonnes pratiques et outils

Objectifs

Dans le cadre de sa mission de certification des comptes, le commissaire aux comptes doit :

1. **Identifier les risques significatifs** liés à la protection des données personnelles susceptibles d'impacter les états financiers,
2. **Évaluer le contrôle interne** mis en place pour assurer la conformité au RGPD, RIA et autres réglementations applicables : le commissaire aux comptes devra notamment vérifier que l'entreprise a réalisé une Analyse d'Impact relative à la Protection des Données pour les technologies d'IA utilisées et qu'elle a mis en place des mesures d'atténuation des risques,

3. **Vérifier la comptabilisation adéquate** des coûts liés à d'éventuelles provisions pour risques,
4. **S'assurer de la pertinence de l'information financière** communiquée dans l'annexe concernant les risques liés à la protection des données.

Bonnes pratiques

Évaluation du niveau de conformité RGPD

Le commissaire aux comptes peut s'appuyer sur le questionnaire d'évaluation suivant :

Thématique	Questions clés	Éléments de preuves à collecter
Gouvernance et accountability	<ul style="list-style-type: none"> - Un Délégué à la Protection des Données (DPO) a-t-il été désigné ? - La documentation requise par le RGPD est-elle à jour ? - Les rôles et responsabilités sont-ils clairement définis ? 	<ul style="list-style-type: none"> - Lettre de mission du DPO - Registre des traitements - Politiques et procédures internes
Gestion des risques	<ul style="list-style-type: none"> - Des analyses d'impact (AIPD) sont-elles réalisées pour les traitements à risque ? - Les risques sont-ils régulièrement réévalués ? - Des audits de conformité sont-ils menés ? 	<ul style="list-style-type: none"> - Rapports d'analyses d'impact - Cartographie des risques - Rapports d'audit
Droits des personnes	<ul style="list-style-type: none"> - Les mentions d'information sont-elles complètes et accessibles ? - Les processus de gestion des demandes d'exercice des droits sont-ils opérationnels ? - Les consentements sont-ils recueillis et conservés ? 	<ul style="list-style-type: none"> - Politiques de confidentialité - Procédures de traitement des demandes - Registres des consentements
Sécurité des données	<ul style="list-style-type: none"> - Des mesures techniques et organisationnelles sont-elles en place ? - Les incidents de sécurité sont-ils détectés et gérés ? - Des tests d'intrusion sont-ils réalisés ? 	<ul style="list-style-type: none"> - Politique de sécurité des SI - Procédure de gestion des incidents - Rapports de tests
Sous-traitance	<ul style="list-style-type: none"> - Les contrats avec les sous-traitants incluent-ils les clauses RGPD ? - Un suivi des sous-traitants est-il assuré ? - Les garanties sont-elles suffisantes ? 	<ul style="list-style-type: none"> - Contrats de sous-traitance - Procédures d'évaluation des sous-traitants - Audits des sous-traitants
Transferts internationaux	<ul style="list-style-type: none"> - Les transferts hors UE sont-ils identifiés ? - Des garanties appropriées sont-elles mises en place ? - Les évolutions réglementaires sont-elles suivies ? 	<ul style="list-style-type: none"> - Cartographie des flux - Clauses contractuelles types - Règles d'entreprise contraignantes

Intégration dans l'approche d'audit

Le commissaire aux comptes intègre l'évaluation de la conformité RGPD dans son approche d'audit par :

1. Phase de planification :

- Identification des traitements de données personnelles significatifs,
- Évaluation préliminaire des risques associés,
- Détermination du niveau d'expertise nécessaire (recours éventuel à un spécialiste).

2. Phase intérimaire :

- Évaluation du contrôle interne lié à la protection des données,
- Tests de procédures sur la gouvernance des données,
- Vérification des processus de gestion des incidents.

3. Phase finale :

- Examen des éventuelles provisions pour risques liés au RGPD,
- Vérification des informations fournies dans l'annexe,
- Évaluation des événements postérieurs à la clôture (incidents, contrôles CNIL, etc.).

Outils & documentations mises à disposition

Pour évaluer les points ci-dessus, le commissaire aux comptes devra mettre en œuvre un **programme de travail ciblé**, s'appuyant à la fois sur des entretiens, des revues documentaires et éventuellement des tests. Parmi les **outils d'audit** et diligences à réaliser, on peut citer :

→ **Entretiens avec les responsables clés** : En premier lieu, rencontrer le DPO (s'il y en a un) ou à défaut un référent RGPD, ainsi que les responsables IT et métiers concernés, afin de comprendre l'organisation mise en place. Ces entretiens permettent de cerner la culture de l'entreprise vis-à-vis des données personnelles, d'identifier les traitements majeurs et de repérer d'éventuels incidents passés.

Par exemple, interroger le DPO sur les principaux risques qu'il a identifiés, sur la fréquence des demandes de droits reçues, sur d'éventuelles plaintes CNIL ou failles de sécurité rencontrées, etc.

→ **Collecte et analyse de la documentation** : Demander et examiner les documents *clés de conformité* :

- Le **registre des traitements** : vérifier qu'il est tenu à jour, complet (finalités, bases légales, catégories de données/personnes, destinataires, durées de conservation, mesures de sécurité, transferts hors UE...) et qu'il couvre bien tous les processus métiers impliquant des données personnelles. Son absence totale serait un signal d'alerte sérieux.

- Les **analyses d'impact (AIPD)** : pour les traitements sensibles identifiés, s'assurer qu'une AIPD a été réalisée conformément à l'article 35 RGPD. Le CAC en fera une revue critique – par exemple, il regardera si les risques résiduels jugés "élevés" ont fait l'objet d'une notification préalable à la CNIL, ou si les mesures d'atténuation recommandées ont été effectivement mises en œuvre.

- Les **politiques et procédures internes** : politique de protection des données ou charte informatique, procédures sur les droits des personnes (modèles de réponse aux demandes d'accès, processus interne pour canaliser ces demandes), procédure de gestion des incidents de sécurité (escalade en 72 h, notification type à la CNIL), plan de continuité d'activité IT en cas de sinistre, etc.

L'idée est de voir si le cadre formel existe et est cohérent avec la réglementation.

Une attention particulière sera portée aux procédures assurant l'exercice des droits des personnes (droits d'information, d'opposition, d'accès, de rectification, d'effacement, de portabilité...) : le CAC peut par exemple tester sur un échantillon comment une demande d'accès serait traitée, ou si des demandes reçues ont bien obtenu réponse dans les délais.

- Les **mentions d'information et contrats** : examiner les modèles de mentions RGPD communiquées aux clients ou utilisateurs (sur le site web, formulaires, CGV/CGU) afin de vérifier qu'elles couvrent les points obligatoires (finalités, droits, contact DPO, base légale...) et ne sont pas trompeuses vis-à-vis des pratiques réelles.

De même, passer en revue les clauses des contrats de sous-traitance les plus critiques pour voir si elles intègrent les engagements requis (confidentialité, aide au responsable de traitement, notification des violations, mesures techniques...).

→ **Cartographie des flux et des systèmes** : Lorsque c'est pertinent, réaliser ou exploiter une cartographie du système d'information et des flux de données personnelles, notamment si l'entité n'en dispose pas formellement.

Cela permet d'identifier des traitements *cachés* ou non documentés (par ex. des exports de données vers un prestataire non mentionné) et de repérer les transferts internationaux.

Le CAC peut demander un schéma des applications utilisées avec les données personnelles qu'elles traitent, et vérifier, pour chaque flux sortant de l'UE, qu'un mécanisme juridique est en place (décision d'adéquation, clauses types signées, BCR, etc.). Cette approche rejoint la vérification de l'inventaire des données, mais sous un angle technique.

→ **Tests de fonctionnement des contrôles** : Selon le risque évalué, l'auditeur peut décider de tester concrètement certains contrôles.

Par exemple, tester l'autorisation des accès : vérifier sur un échantillon d'utilisateurs que leurs droits d'accès aux applications métiers manipulant des données personnelles respectent bien la règle du *moindre privilège* (besoin d'en connaître).

Ou simuler une demande d'exercice de droit (droit d'accès) pour voir si l'entreprise répond dans les délais et de manière conforme.

Ou encore examiner le journal des incidents de sécurité pour voir s'ils ont été correctement catégorisés et s'il n'y a pas eu d'omission de notification alors qu'un incident le requerrait.

Si l'entité utilise un outil de gestion des consentements cookies/traceurs, le CAC peut vérifier son paramétrage (ex. est-ce que le dépôt de cookies non essentiels est bien bloqué avant consentement ?).

Ces tests fournissent des preuves tangibles du niveau d'application des procédures affichées.

→ **Revue des mesures techniques de sécurité** : Impliquer éventuellement l'auditeur IT ou s'aider de questionnaires techniques pour évaluer le niveau de sécurité lié aux données personnelles.

Par exemple, contrôler que les postes de travail avec accès à des données sensibles sont chiffrés, que des sauvegardes chiffrées sont réalisées régulièrement, que les mises à jour logicielles sont déployées (pour éviter des vulnérabilités exploitées par des attaquants), ou encore que des tests d'intrusion ou analyses de vulnérabilités sont effectués périodiquement sur les systèmes critiques. On se référera aux guides de l'ANSSI et de la CNIL en la matière (*guide de sécurité des données personnelles* de la CNIL, etc.).

L'ensemble de ces démarches vise à recueillir suffisamment d'éléments probants pour étayer l'opinion de l'auditeur sur le niveau de risque résiduel.

Tous les constats (forces et faiblesses) seront consignés dans le dossier de travail, avec leurs impacts potentiels.

Si nécessaire, le CAC pourra alerter les organes de gouvernance sur un risque de non-conformité sérieux (par exemple, absence de toute procédure alors même que des données sensibles sont exploitées), ce qui pourrait relever d'une faiblesse significative du contrôle interne.

Impact dans la stratégie du commissaire aux comptes

L'évaluation des risques liés à la protection des données personnelles influence la stratégie d'audit :

1. **Ajustement du seuil de signification** : en fonction de l'exposition aux risques RGPD et des enjeux associés,
2. **Orientation des travaux** : concentration sur les zones de risque identifiées (secteurs sensibles, traitements massifs, transferts internationaux, secteurs médico-social et associatif),
3. **Communication avec les organes de gouvernance** : alerte sur les risques significatifs identifiés lors des travaux,
4. **Approche pluriannuelle** : suivi de l'évolution de la maturité RGPD de l'entité,
5. **Proposition de SACC** : en fonction des besoins identifiés et dans le respect des règles d'indépendance (Diagnostic de maturité ou audit de compliance ?).

Séquence 3

Cas d'usage

Évaluation de la conformité RGD d'une PME du secteur e-commerce

Contexte

La société WebShop SA est une PME de 45 salariés spécialisée dans la vente en ligne de produits cosmétiques. Elle réalise un chiffre d'affaires de 8,5 millions d'euros, dont 30% à l'international.

La société dispose d'une base de données clients de plus de 150 000 contacts et utilise des outils marketing avancés (CRM, emailing, ciblage publicitaire).

Identification des risques par le commissaire aux comptes

1. Lors de la prise de connaissance :

- Traitement de données clients à grande échelle,
- Collecte de données de paiement,
- Transferts de données vers des prestataires aux États-Unis (hébergement cloud, outils marketing),
- Absence de DPO désignée,
- Utilisation intensive de cookies et traceurs sur le site web.

2. Évaluation du contrôle interne :

- Registre des traitements incomplet,
- Absence d'analyses d'impact pour les traitements à risque,
- Mentions d'information non conformes sur le site web,
- Contrats de sous-traitance non mis à jour post-RGD,
- Absence de procédure formalisée de gestion des violations de données.

3. Évaluation des impacts financiers potentiels :

- Risque d'amendes administratives (jusqu'à 4% du CA mondial),
- Coûts de mise en conformité non provisionnés,
- Absence d'information dans l'annexe sur les risques RGD.

Approche d'audit adaptée

1. Travaux complémentaires :

- Examen approfondi des contrats avec les sous-traitants hors UE,
- Vérification des mécanismes de recueil du consentement,

- Évaluation de la sécurité des données de paiement,
- Examen des processus de gestion des droits des personnes.

2. Communication avec la gouvernance :

- Point spécifique sur les risques RGD lors de la réunion de synthèse,
- Recommandation de désigner un DPO ou référent RGD,
- Alerte sur les transferts hors UE non sécurisés (post-Schrems II).

3. Impact sur l'opinion :

- Incorporation des risques RGD dans l'évaluation globale des risques,
- Vérification de l'absence d'impact significatif sur les comptes,
- Recommandation d'information dans l'annexe sur les risques liés à la protection des données.

Proposition de prestations

Le commissaire aux comptes propose une mission d'accompagnement à la mise en conformité RGD, incluant :

- L'établissement d'une cartographie complète des traitements,
- L'évaluation détaillée des risques pour les droits et libertés des personnes,
- La validation de la mise à jour des mentions d'information et politiques,
- L'évaluation des risques liés aux contrats de sous-traitance conclus par l'entreprise.

Checklist pratique pour l'audit des enjeux RGD dans une PME e-commerce

- Vérifier l'existence et la complétude du registre des traitements,
- Examiner les mentions d'information sur le site web (politique de confidentialité),
- Contrôler les mécanismes de recueil du consentement (cookies, prospection),
- Évaluer la sécurité des données sensibles (paiement, coordonnées),
- Vérifier les contrats avec les prestataires hébergeant des données,
- Examiner la localisation des données et les transferts internationaux,
- Contrôler les procédures de réponse aux demandes d'exercice des droits,
- Évaluer les mesures de sécurité techniques et organisationnelles,
- Vérifier l'existence d'une procédure de gestion des violations de données,
- Examiner la formation et la sensibilisation des collaborateurs.

Séquence 4

Allez plus loin

Ressources pratiques

- Guide CNIL sur la tenue du registre des traitements : <https://www.cnil.fr/fr/rgpd-et-tpepme-comment-tenir-votre-registre-de-traitement>
- Modèles de clauses contractuelles types pour les transferts internationaux : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_fr
- Lignes directrices du Comité Européen de la Protection des Données (CEPD) : https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_fr
- Outil PIA de la CNIL pour les analyses d'impact : <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>
- Référentiel CNIL sur les durées de conservation : <https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees>

Formations recommandées

- CNCC - Protection des données personnelles : enjeux pour le commissaire aux comptes
- CRCC - Audit informatique et conformité réglementaire
- CNIL - Délégué à la protection des données : formation de base
- AFAI/ISACA - Audit de la gouvernance des données

Évolutions réglementaires à surveiller

- Application du Data Governance Act qui établit un cadre pour faciliter le partage des données
- Mise en œuvre du Data Act qui vise à réguler l'économie des données en Europe
- Évolution de la jurisprudence post-Schrems II concernant les transferts internationaux
- Nouvelles lignes directrices du CEPD sur l'intelligence artificielle et les données personnelles
- NIS / NIS 2
- RIA