# Checklist RGPD pour le SMQ

Ce que les qualiticiens doivent savoir — Mai 2026

**Ressource gratuite**

ISOthèque — isotheque.fr · FR-QUA-RGPD-01 | v1.0

# Checklist RGPD pour le SMQ — Ce que les qualiticiens doivent savoir

**Ressource gratuite ISOthèque — isotheque.fr Réf. : FR-QUA-RGPD-01 | v1.0 | Mai 2026 Applicable aux organismes établis dans l'Union Européenne**

Le RGPD (Règlement Général sur la Protection des Données) et l'ISO 9001:2015 se croisent plus souvent qu'on ne le pense. Les qualiticiens collectent, traitent et conservent des données personnelles dans le cadre du SMQ — données salariés, données clients, enregistrements d'audits, réclamations — sans toujours avoir vérifié que ces traitements sont conformes au RGPD.

Cette checklist vous permet de faire un point rapide sur les principaux points de conformité RGPD dans le contexte du SMQ. Elle ne remplace pas un audit RGPD complet ni un avis juridique, mais elle permet d'identifier les lacunes les plus fréquentes.

**Légende :**

- ■ **Conforme** — la disposition est en place et documentée
- ■ **À vérifier** — la situation n'est pas claire ou non documentée
- ✗ **Non conforme** — la disposition est absente

## PARTIE 1 — Les données personnelles dans le SMQ

### 1.1 Identification des données traitées

■ ■ **Nous avons identifié les catégories de données personnelles traitées dans le cadre du SMQ :**

- Données salariés : noms, fonctions, habilitations, formations, évaluations de compétences
- Données clients : noms de contacts, emails, téléphones, historique de réclamations
- Données fournisseurs : contacts nominatifs, évaluations individuelles
- Données d'audit : noms des audités, personnes citées dans les rapports
- Données de non-conformités : personnes impliquées, témoignages

■ ■ **Un registre des activités de traitement (RAT) a été établi**, listant pour chaque traitement : finalité, catégories de données, personnes concernées, durées de conservation, destinataires, mesures de sécurité.

■ ■ **Les traitements sans base légale identifiée ont été signalés** au responsable de traitement (direction).

> ***Point d'attention SMQ :*** *les rapports d'audit, les fiches de NC et les registres de réclamations contiennent souvent des données personnelles (noms d'opérateurs, de clients, d'auditeurs). Ces documents doivent être traités comme des données personnelles et leur conservation doit être justifiée.*

### 1.2 Bases légales des traitements

Pour chaque traitement de données personnelles, une base légale doit être identifiée parmi les 6 prévues par l'article 6 du RGPD :

- ■ **Données salariés dans le SMQ** (habilitations, compétences, formations) → Base légale : **obligation légale** (droit du travail, obligations de sécurité) ou **exécution du contrat de travail**. Ces données ne nécessitent pas de consentement.
- ■ **Données clients dans les réclamations** (nom, email, historique) → Base légale : **intérêt légitime** (traiter les réclamations est légitime) ou **exécution du contrat**. Une réclamation implique une relation contractuelle.
- ■ **Données dans les évaluations fournisseurs** (contacts nominatifs) → Base légale : **intérêt légitime**. L'évaluation de la performance des fournisseurs est légitime dans le cadre commercial.
- ■ **Données dans les audits internes** (noms des personnes auditées) → Base légale : **intérêt légitime** ou **obligation légale** (pour les audits réglementaires).

> ***Ce qu'il ne faut pas faire :*** *collecter le consentement pour des traitements qui ont déjà une base légale. Cela crée une complexité inutile et un risque si le consentement est retiré.*

---

## PARTIE 2 — Durées de conservation

### 2.1 Durées définies et respectées

- ■ **Les durées de conservation sont définies pour chaque catégorie d'enregistrements du SMQ** dans la procédure de maîtrise documentaire ou dans le registre des activités de traitement.

Durées recommandées pour les données personnelles dans le SMQ :

| Type d'enregistrement | Durée recommandée | Base légale conservation |
|---|---|---|
| Dossiers de formation et habilitations salariés | Durée du contrat + 5 ans | Preuve de compétence §7.2 + prescription sociale |
| Rapports d'audit interne (avec noms) | 5 ans | §9.2 ISO 9001 + intérêt légitime |
| Fiches de non-conformité (avec noms) | 5 ans | §10.2 ISO 9001 + intérêt légitime |
| Réclamations clients (avec données contact) | 5 ans | Prescription commerciale (art. L.110-4 Code commerce) |
| Évaluations fournisseurs (contacts nominatifs) | Durée relation + 3 ans | Intérêt légitime |
| Comptes rendus de revue de direction | 5 ans | §9.3 ISO 9001 |

| Type d'enregistrement | Durée recommandée | Base légale conservation |
|---|---|---|
| Enquêtes de satisfaction clients | 3 ans | Intérêt légitime |

- ■ **Un processus de purge ou d'anonymisation est en place** pour supprimer ou anonymiser les données à l'issue de la durée de conservation.
- ■ **Les versions obsolètes de documents contenant des données personnelles sont détruites** de façon sécurisée (pas simplement déplacées dans un dossier "archives" accessible à tous).

---

# PARTIE 3 — Information des personnes concernées

## 3.1 Transparence vis-à-vis des salariés

- ■ **Les salariés ont été informés** des traitements de données les concernant dans le cadre du SMQ (habilitations, audits, fiches NC). Cette information peut figurer dans :
  - Le règlement intérieur
  - Une note d'information RGPD remise à l'embauche
  - La politique de confidentialité interne
- ■ **Les salariés savent comment exercer leurs droits** (accès, rectification, effacement dans les limites des obligations légales) et à qui s'adresser.

> ***Point pratique :*** *un salarié peut demander à consulter les données personnelles qui le concernent dans les rapports d'audit ou les fiches NC. Il ne peut pas demander la suppression si la conservation répond à une obligation légale ou à un intérêt légitime documenté.*

## 3.2 Transparence vis-à-vis des clients

- ■ **Les clients sont informés** du traitement de leurs données personnelles dans le cadre de la gestion des réclamations et des enquêtes de satisfaction (mention dans les CGV, email de confirmation, formulaire de réclamation).
- ■ **La politique de confidentialité du site web est accessible** et mentionne le traitement des données clients dans le contexte des réclamations.

---

# PARTIE 4 — Sécurité des données

## 4.1 Mesures de sécurité en place

- ■ **L'accès aux enregistrements du SMQ contenant des données personnelles est restreint** aux personnes ayant besoin d'y accéder dans le cadre de leurs fonctions. Les droits d'accès sont définis et documentés.
- ■ **Les documents physiques** (fiches NC papier, rapports d'audit imprimés) sont conservés dans des espaces sécurisés (armoires fermées à clé, local dédié).

- ■ **Les documents numériques** sont stockés sur des serveurs ou systèmes dont l'accès est contrôlé (authentification, droits par rôle, journaux d'accès si applicable).
- ■ **Les prestataires extérieurs** ayant accès aux données personnelles du SMQ (consultants qualité, auditeurs externes, organismes de certification) sont liés par un contrat ou une clause de confidentialité.
- ■ **L'organisme de certification** a accès à des données personnelles lors des audits (noms des audités, données dans les enregistrements). Vérifier que leur contrat inclut les clauses RGPD appropriées (sous-traitance de données).

### 4.2 Violations de données

- ■ **Une procédure de gestion des violations de données** est définie : qui est notifié, dans quel délai (72h pour la CNIL si risque élevé), comment documenter l'incident.
- ■ **Les personnes référentes** en cas de violation de données sont identifiées (direction, DPO si applicable, responsable qualité).

---

## PARTIE 5 — Droits des personnes

### 5.1 Exercice des droits

- ■ **Un canal de contact est défini** pour l'exercice des droits RGPD (email dédié, formulaire en ligne, ou adresse postale clairement communiquée).
- ■ **Le délai de réponse d'un mois maximum** est connu et respecté par les personnes en charge de traiter les demandes.
- ■ **Les demandes d'exercice de droits sont tracées** (date de réception, nature de la demande, réponse apportée, date de réponse).

Les droits à connaître dans le contexte du SMQ :

| Droit | Application SMQ | Limite possible |
|---|---|---|
| Accès (art. 15) | Un salarié peut demander ses données dans les dossiers qualité | Données relatives à d'autres personnes à occulter |
| Rectification (art. 16) | Corriger une erreur factuelle dans une fiche | Ne s'applique pas aux constats d'audit déjà validés |
| Effacement (art. 17) | Limité si obligation légale de conservation | Non applicable si durée légale en cours |
| Opposition (art. 21) | Pour les traitements basés sur l'intérêt légitime | L'organisme peut refuser si intérêt légitime prédomine |
| Portabilité (art. 20) | Ne s'applique pas aux données salariés SMQ en général | Uniquement pour consentement ou contrat |

---

# PARTIE 6 — Points spécifiques au SMQ

## 6.1 Les audits internes et le RGPD

- ■ **Les rapports d'audit ne citent pas de personnes nominativement de façon disproportionnée.** Les constats portent sur les processus et les systèmes, pas sur les individus. Si des noms apparaissent, c'est justifié par la traçabilité nécessaire.
- ■ **L'accès aux rapports d'audit est limité** aux personnes ayant un besoin légitime (responsable qualité, direction, auditeurs). Ils ne sont pas partagés librement.
- ■ **Lors de la transmission de rapports d'audit à l'organisme de certification**, les données personnelles non nécessaires à la certification peuvent être anonymisées.

## 6.2 Les réclamations clients et le RGPD

- ■ **Les données clients dans le registre des réclamations** (nom, email, téléphone, description du problème) sont traitées selon le principe de minimisation : seules les données nécessaires au traitement de la réclamation sont collectées.
- ■ **Les réclamations anciennes** (au-delà de la durée de conservation définie) sont supprimées ou anonymisées régulièrement.
- ■ **Les données de réclamations ne sont pas utilisées à des fins commerciales** sans base légale appropriée (consentement, si applicable).

## 6.3 Les prestataires et sous-traitants accédant au SMQ

- ■ **Consultants qualité externes** : ont-ils signé un accord de confidentialité / une clause de sous-traitance de données ?
- ■ **Organisme de certification** : le contrat inclut-il les clauses RGPD pour les données auxquelles leurs auditeurs ont accès ?
- ■ **Logiciels de gestion qualité (GMAO, logiciel de suivi NC, GED)** : avez-vous signé un DPA (Data Processing Agreement) avec les éditeurs hébergeant vos données ?

---

# PARTIE 7 — Gouvernance RGPD

## 7.1 Responsabilités

- ■ **Un responsable de traitement est clairement identifié** (généralement la direction de l'organisme). C'est lui qui répond légalement des traitements de données.
- ■ **La désignation d'un DPO (Délégué à la Protection des Données)** a été évaluée. Elle est obligatoire pour les organismes publics, les organismes traitant à grande échelle des données sensibles, ou ceux réalisant une surveillance systématique à grande échelle. Pour la plupart des PME, elle est facultative mais recommandée.
- ■ **Le responsable qualité connaît ses obligations RGPD** dans le cadre du SMQ et sait à qui escalader en cas de doute.

## 7.2 Lien RGPD / ISO 9001

Le RGPD peut être intégré au SMQ comme une **exigence applicable** au sens du §4.2 (parties intéressées — les personnes concernées par les traitements de données) et du §6.1 (risques — le risque de non-conformité RGPD est un risque réel pour l'organisme).

- ■ **La conformité RGPD est intégrée à l'analyse des risques du SMQ** (§6.1).
- ■ **Les violations de données constituent des non-conformités potentielles** traitées selon la procédure §10.2.
- ■ **La conformité RGPD est un sujet de la revue de direction** (§9.3.2 — enjeux externes et contexte de l'organisme).

---

## Résumé des points les plus critiques

Les 5 points qui concentrent la plupart des non-conformités RGPD dans les SMQ :

**1. Absence de registre des activités de traitement (RAT) — obligatoire pour tout organisme de plus de 250 salariés, fortement recommandé pour tous.**

**2. Durées de conservation non définies — les enregistrements du SMQ sont conservés indéfiniment "au cas où". C'est une violation du principe de limitation de la conservation.**

**3. Accès non restreint aux enregistrements — tout le monde peut consulter les fiches NC, les rapports d'audit, le registre des réclamations. Les droits d'accès doivent être définis.**

**4. Prestataires sans clause RGPD — consultants qualité, organisme de certification, éditeur de logiciel qualité accédant aux données sans contrat approprié.**

**5. Absence d'information des salariés — les salariés ne savent pas que leurs données (habilitations, évaluations, présence dans les rapports d'audit) sont traitées dans le SMQ.**

---

## Ressources utiles

- **CNIL** — cnil.fr — Autorité de contrôle française, guides pratiques gratuits
- **Référentiel RGPD CNIL pour les TPE/PME** — cnil.fr/fr/rgpd-et-tpe-pme
- **Registre des activités de traitement** — modèle CNIL disponible gratuitement
- **Plateforme de plainte CNIL** — cnil.fr/fr/plaintes

---

*Cette checklist est un outil de sensibilisation. Elle ne constitue pas un avis juridique et ne remplace pas une analyse RGPD complète réalisée par un professionnel qualifié. En cas de doute sur votre conformité, consultez un DPO externe ou un avocat spécialisé en protection des données.*


*Réf. : FR-QUA-RGPD-01 | v1.0 | Mai 2026*

*Tags : RGPD, protection des données, SMQ, ISO 9001, données personnelles, audit RGPD, qualiticiens*

---