



COMPLYSHIELD

Ressource gratuite · fondée sur sources officielles CNIL

À faire avant un contrôle CNIL

Une preuve attendue par point

Checklist RGPD express pour PME

12 points à vérifier avant un contrôle CNIL

Objectif : réunir rapidement les preuves minimales sur vos traitements, votre information, vos sous-traitants, vos cookies, votre sécurité et votre procédure incident.

Mode d'emploi 20 minutes

Cochez uniquement si une preuve existe.
Sinon : responsable + échéance sous 30 jours.

01 Registre

Lister les traitements réels : clients, prospects, RH,
 ☒ Registre daté, propriétaire interne, finalité par ligne,
 ☒ diffuseurs, site web.

02 Base légale

Associer chaque finalité à une base légale adaptée, pas
 ☒ Contrat, obligation légale, intérêt légitime, consentement...
 ☒ Consentement par réflexe.

03 Information

Vérifier les mentions sur formulaires, devis, collecte RH
 ☒ Texte clair : finalité, droits, contact, durées, destinataires.
 ☒ Politique de confidentialité.

04 Droits

Prévoir comment répondre aux demandes d'accès,
 ☒ Canal de contact, responsable, journal des demandes et
 ☒ justification, opposition, enlèvement, réponses.

05 Conservation

Définir des durées concrètes et supprimer les données
 ☒ Tableau de durées + règle de purge ou archivage.
 ☒ Données inutiles.

06 Sous-traitants

Identifier CRM, hébergeur, emailing, paie, analytics et
 ☒ Contrats/DPA, instructions, sécurité, transferts éventuels.
 ☒ Adresser leurs obligations.

07 Cookies

Bloquer les traceurs non essentiels tant que le
 ☒ Bandeau, preuve du choix, bouton refuser aussi simple
 ☒ que l'accepter.
 ☒ Si le consentement n'est pas donné.

08 Sécurité

Réduire le risque : accès nominatif, MFA, mots de passe
 ☒ Politique simple + preuve des comptes et habilitations.
 ☒ Les sauvegardes, mises à jour.

09 Violation

Savoir qualifier une fuite et notifier la CNIL sous 72h si le
 ☒ Procédure incident, contacts, modèle de notification,
 ☒ registre incidents.

10 AIPD

Repérer les traitements à risque élevé : données
 ☒ Décision documentée : AIPD requise ou non, avec
 ☒ simples, surveillance, scoring, volume massif,
 ☒ justification.

11 Transferts

Contrôler les outils hors UE et le mécanisme
 ☒ Pays, prestataire, base de transfert, information des
 ☒ personnes.
 ☒ Cadre réglementaire utilisé.

12 Preuves

Centraliser les preuves avant contrôle : versions,
 ☒ Dossier RGPD partagé, revu chaque trimestre ou à chaque
 ☒ nouvelles mesures, contrats, décisions, revues.
 ☒ nouveau outil.

Sources CNIL utilisées

[CNIL — Le registre des activités de traitement](#)
[CNIL — Sécurité des données personnelles](#)

[CNIL — Violations de données personnelles](#)
[CNIL — Les droits des personnes](#)

[CNIL — Cookies et autres traceurs](#)

Kit RGPD PME

Registre CSV, checklist 30 points
et procédure 72h.

Kit 39 €