

RGPD, cybersécurité et données politiques - v1.0

Politique de conformité et sécurité prête à implémentation

Mise à jour : 27 septembre 2026

Niveau de sensibilité. Le fait même d'être enregistré comme adhérent d'un parti révèle une opinion politique. Ces données sont sensibles et nécessitent une gouvernance stricte.

1. Gouvernance des données

- Nommer un responsable interne protection des données et déterminer si la désignation formelle d'un DPO est obligatoire ou opportune.
- Tenir un registre de traitements.
- Réduire les données collectées au strict nécessaire.
- Définir des durées de conservation par finalité.
- Documenter les bases juridiques et exceptions de l'article 9 RGPD utilisées.

2. Traitements principaux

Traitement	Données	Finalité	Mesures clés
Adhérents	Identité, contact, cotisation, historique minimal	Gestion du membership	RBAC, chiffrement, journalisation
Donateurs	Identité, montant, justificatifs	Conformité financière	Accès restreint, conservation légale
Sympathisants	Contact, consentements/opposition	Information politique	Désinscription immédiate
Candidats	Identité, déclarations, pièces d'éligibilité	Investiture	Accès limité, purge après durée définie
Signalements	Faits, pièces, personnes	Éthique/compliance	Coffre chiffré, accès comité limité

3. AIPD

Une analyse d'impact est obligatoire lorsqu'un traitement est susceptible d'engendrer un risque élevé. Compte tenu des données politiques sensibles, de possibles traitements à grande échelle, du ciblage ou de techniques nouvelles, le Parti doit réaliser une analyse formelle avant le lancement des traitements présentant ces caractéristiques.

4. Sécurité minimale

- MFA obligatoire pour les comptes administrateurs.
- Gestionnaire de mots de passe organisationnel.
- Chiffrement au repos et en transit.
- Sauvegardes chiffrées et restaurations testées.
- Journalisation des accès aux données sensibles.

- Principe du moindre privilège.
- Revue trimestrielle des droits.
- Mises à jour et inventaire des actifs.
- Plan de réponse à incident et procédure de notification CNIL si applicable.

5. Hébergement

Les données politiques les plus sensibles sont hébergées selon une analyse de risque intégrant localisation, droit applicable, chiffrement, réversibilité, sous-traitants et capacité d'audit. Le choix d'un fournisseur français ou européen ne dispense pas d'un audit de sécurité.

6. Prospection politique

Toute personne contactée doit être informée de l'identité du responsable, de la finalité, de la source des données lorsque requise et de ses droits, dont l'opposition aux sollicitations futures. Le ciblage politique en ligne nécessite en plus le respect des règles spécifiques de transparence applicables.

7. Mineurs

Si le Parti accepte l'adhésion de mineurs dans les limites légales, un parcours d'information spécifique est prévu et la collecte de données est strictement minimisée.

8. Incident

1. Isoler le système concerné.
2. Préserver les journaux et preuves.
3. Évaluer type de données, volume et personnes touchées.
4. Décider des notifications réglementaires dans les délais applicables.
5. Informer les personnes lorsque le risque l'exige.
6. Corriger la cause et publier un retour d'expérience interne.

9. Matrice de droits

Rôle	Adhérents	Donateurs	Signalements	Exports
Admin SI	Technique seulement	Technique seulement	Non sauf besoin	Contrôlé
Adhésions	Oui	Non	Non	Limité
Mandataire/finance	Minimal	Oui	Non	Finance seulement
Éthique	Minimal	Non	Oui	Non
Communication	Opt-in/contacts autorisés	Non par défaut	Non	Contacts seulement

Sources juridiques et institutionnelles principales

- **CNIL - fichiers de communication politique:** <https://www.cnil.fr/fr/les-fichiers-de-communication-politique>
- **CNIL - AIPD:** <https://www.cnil.fr/fr/ce-qui-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>

Note : les références sont données comme points de contrôle. Avant dépôt, campagne ou collecte de fonds, une revue juridique actualisée reste nécessaire.