Fiche méthode 1 : Démarche de conformité au RGPD

**Comment s'y prendre pour assurer la conformité au RGPD d'une organisation** **?**

Par où commencer ? Quelles sont les éléments obligatoires ? Quels sont ceux qui ne seront mis en œuvre que dans certains contextes.

Cette fiche répond à toutes ces questions de façon synthétique. Elle doit être complétée par des ressources en lignes ou par d'autres fiches pour étudier chacun des points.

Elle présente dans un premier temps la démarche globale : les étapes à faire dans tous les cas sont mises en évidence (**gras et surligné**).

Des questions spécifiques sont ensuite étudiées, toujours de façon synthétique.

[I Démarche globale 2](#_Toc51681274)

[II Questions spécifiques 5](#_Toc51681275)

[1 Relations avec les Clients 5](#_Toc51681276)

[2 Relation avec les salariés 5](#_Toc51681277)

[3 Communication / Vente en ligne 6](#_Toc51681278)

 

**Sources** :

MOOC RGPD de la CNIL : <https://atelier-rgpd.cnil.fr/> (à venir)

=> FS0 MOOC RGPD (copies d'écrans)

<https://www.cnil.fr/rgpd-passer-a-laction>

<https://www.cnil.fr/fr/rgpd-par-ou-commencer>

<https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf>

<https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes>

#### Démarche globale

|  |  |  |
| --- | --- | --- |
| **ETAPE** | **EXPLICATIONS** | **RESSOURCES** |
| Piloter | Désigner un pilote RGPD, éventuellement un DPO | <https://www.cnil.fr/fr/designer-un-pilote> |
| **Cartographier** | Recenser les traitements sur les données personnelles   * Qui est responsable ? * Quelle est la nature des données ? Base légale ? * Pourquoi sont-elles collectées ? * Où sont-elles stockées ? * Jusqu'à quand ? * Quelles sont les mesures de sécurité ? | <https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles>  <https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement>  <https://www.cnil.fr/sites/default/files/atoms/files/registre-traitement-simplifie.ods>  <https://www.cnil.fr/fr/les-bases-legales> |
| **Faire le tri** | Vérifier les règles de bases concernant les données :   * finalité affichées à la collecte * minimiser les données * identifier les données à risque | <https://www.cnil.fr/fr/prioriser-les-actions-mener> |
| **Respecter les droits**  info + accès | Informer les personnes de façon transparente et recueillir leur consentement  Assurer les droits des personnes   * accès, rectification, opposition, suppression des données * portabilité, limitation, intervention humaine | <https://www.cnil.fr/fr/respecter-les-droits-des-personnes>  <https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation> |

|  |  |  |
| --- | --- | --- |
| **Sécuriser les données** | Assurer la confidentialité, la disponibilité, l'intégrité et les conditions de preuve  Proportionner les mesures aux risques : vraisemblance / gravité & impact   * N1 règles de bonne pratique * N2 mesures d'hygiène * N3 gérer les risques   + vraisemblance : menace / source / scénario   + gravité : impact   + mesures : prévention / protection / détection / réaction | <https://www.cnil.fr/fr/securite-des-donnees>  check list : <https://www.cnil.fr/sites/default/files/atoms/files/check_list_0.pdf>  <https://www.cybermalveillance.gouv.fr/>  N1 Les bonnes pratiques minimales  <https://www.cnil.fr/fr/securite-des-donnees-les-regles-essentielles-pour-demarrer>  <https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/>  N2 Bonnes pratiques avancées  <https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>  <https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf>  N3  <https://www.cnil.fr/fr/securite-des-donnees-proteger-le-plus-sensible-de-maniere-specifique> <https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/> |
| Gérer les données à risque | Une analyse d'impact sur la protection des données est obligatoire quand les risques sont élevés pour les droits et la vie privée. | <https://www.cnil.fr/fr/gerer-les-risques>  <https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd>  <https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>  Outil : PID  <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>  Guides   * [la méthode](https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf) * [les modèles](https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf) * [les bases de connaissances](https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf) * un exemple : [le cas Captoo](https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-captoo-fr.pdf) |

|  |  |  |
| --- | --- | --- |
| **Organiser**  **& Sensibiliser** | En interne :   * prendre en compte la protection des données dès la conception ; * sensibiliser :   + plan de formation,   + charte informatique,   + engagement de confidentialité.   En externe :   * procédures de traitement des réclamations et des demandes ; * procédures en cas de violation des données. | <https://www.cnil.fr/fr/organiser-les-processus-internes>  <https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs> |
| Documenter  = synthèse | Être capable de prouver en temps réel la conformité au RGPD. | <https://www.cnil.fr/fr/documenter-la-conformite>  <https://www.cnil.fr/sites/default/files/atoms/files/formulaire_de_demande_labels-gouvernance-re.docx> |

#### Questions spécifiques

##### Relations avec les Clients

<https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf> pp. 33 à 39

|  |  |  |
| --- | --- | --- |
| Prospecter de clients | **opt-in** : cas où il est nécessaire d'obtenir l'accord avant de contacter le prospect. B2C par email, SMS, MMS, automate d'appel  **opt-ou** : cas où on peut si le prospect ne s'y est pas opposé. B2B par email ou B2C par voie postale ou par téléphone.  Toujours donner la possibilité de refuser de nouvelles sollicitations | <https://pro.bloctel.fr/> |
| Fidéliser | **Faire le tri**  **Informer**  **Ne pas conserver indéfiniment** |  |

##### Relation avec les salariés

<https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf> pp. 40 à 46

<https://www.cnil.fr/sites/default/files/atoms/files/travail-vie_privee.pdf>

Domaines particuliers :

* gestion et recrutement des salariés
* géolocalisation des véhicules
* outils informatiques au travail
* accès aux locaux et contrôle des horaires
* vidéosurveillance
* écoute et enregistrement des appels

##### Communication / Vente en ligne

<https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf> pp. 48 à 54

<https://www.cnil.fr/sites/default/files/atoms/files/commerce_et_donnees_personelles.pdf> (document avant RGPD)

|  |  |  |
| --- | --- | --- |
| Sécuriser | Chiffrer les échanges (https)  Demander un mot de passe complexe  Ne pas envoyer de données personnelles par email  Sécuriser le paiement  Ne pas conserver les données bancaires | <https://www.cnil.fr/fr/securite-securiser-les-sites-web>  <https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/>  <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf> p. 103 sécurité des sites web  => <https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Securite_Web_NoteTech.pdf>  Autre :  <https://www.cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux>  <https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite> |
| Informer | Mentions légales, conditions générales de vente  Page « Politique de confidentialité » | <https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation>  <https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228> |
| Droits des personnes | Proposer des modalités simples de contact  Permettre l'exercice des droits |  |
| Gestion des cookies | Type de cookie :   * technique (panier) => informer * suivi => demander le consentement   Demander le consentement pour les fonctionnalités venant d'autres sites (Google, Facebook…) | <https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs>  <https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite>  <https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-maitriser-votre-navigateur>  Approfondir :  <https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles>  [https://www.cnil.fr/sites/default/files/atoms/files/ projet\_de\_recommandation\_cookies\_et\_autres\_traceurs.pdf](https://www.cnil.fr/sites/default/files/atoms/files/projet_de_recommandation_cookies_et_autres_traceurs.pdf) |