

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
II	Questions spécifiques	5
1	Relations avec les Clients	5
2	Relation avec les salariés	5
3	Communication / Vente en ligne	6

LES 6 BONNS RÉFLEXES DE LA PROTECTION DES DONNÉES PERSONNELLES

1 Ne collectez que les données vraiment nécessaires
Posez-vous les bonnes questions : Quel est mon objectif ?
Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ?
Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?

2 Soyez transparent
Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes dont vous traitez les données.

3 Pensez aux droits des personnes
Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.

4 Gardez la maîtrise de vos données
Le partage et la circulation des données personnelles doivent être encadrées et contractualisées, afin de leur assurer une protection à tout moment.

5 Identifiez les risques
Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer.

6 Sécurisez vos données
Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

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>

I 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 <ul style="list-style-type: none">• 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 : <ul style="list-style-type: none">• 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	Informar les personnes de façon transparente et recueillir leur consentement Assurer les droits des personnes <ul style="list-style-type: none">• 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	<p>Assurer la confidentialité, la disponibilité, l'intégrité et les conditions de preuve</p> <p>Proportionner les mesures aux risques : vraisemblance / gravité & impact</p> <ul style="list-style-type: none"> • N1 règles de bonne pratique • N2 mesures d'hygiène • N3 gérer les risques <ul style="list-style-type: none"> ○ vraisemblance : menace / source / scénario ○ gravité : impact ○ mesures : prévention / protection / détection / réaction 	<p>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/</p> <p>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/</p> <p>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</p> <p>N3 https://www.cnil.fr/fr/securite-des-donnees-protger-le-plus-sensible-de-maniere-specifique https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/</p>
Gérer les données à risque	<p>Une analyse d'impact sur la protection des données est obligatoire quand les risques sont élevés pour les droits et la vie privée.</p>	<p>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</p> <p>Outil : PID https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil</p> <p>Guides</p> <ul style="list-style-type: none"> • la méthode • les modèles • les bases de connaissances • un exemple : le cas Captoo

Organiser & Sensibiliser	<p>En interne :</p> <ul style="list-style-type: none"> • prendre en compte la protection des données dès la conception ; • sensibiliser : <ul style="list-style-type: none"> ○ plan de formation, ○ charte informatique, ○ engagement de confidentialité. <p>En externe :</p> <ul style="list-style-type: none"> • procédures de traitement des réclamations et des demandes ; • procédures en cas de violation des données. 	<p>https://www.cnil.fr/fr/organiser-les-processus-internes https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs</p>
Documenter = synthèse	Être capable de prouver en temps réel la conformité au RGPD.	<p>https://www.cnil.fr/fr/documenter-la-conformite https://www.cnil.fr/sites/default/files/atoms/files/formulaire_de_demande_labels-gouvernance-re.docx</p>

II Questions spécifiques

1 Relations avec les Clients

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnll-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-out : 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 Informé Ne pas conserver indéfiniment	

2 Relation avec les salariés

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnll-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

3 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_personnelles.pdf (document avant RGPD)

Sécuriser	<p>Chiffrer les échanges (https)</p> <p>Demander un mot de passe complexe</p> <p>Ne pas envoyer de données personnelles par email</p> <p>Sécuriser le paiement</p> <p>Ne pas conserver les données bancaires</p>	<p>https://www.cnil.fr/fr/securite-securiser-les-sites-web</p> <p>https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/</p> <p>https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf p. 103 sécurité des sites web</p> <p>=> https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Securite_Web_NoteTech.pdf</p> <p>Autre :</p> <p>https://www.cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux</p> <p>https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite</p>
Informé	<p>Mentions légales, conditions générales de vente</p> <p>Page « Politique de confidentialité »</p>	<p>https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation</p> <p>https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228</p>
Droits des personnes	<p>Proposer des modalités simples de contact</p> <p>Permettre l'exercice des droits</p>	
Gestion des cookies	<p>Type de cookie :</p> <ul style="list-style-type: none"> technique (panier) => informer suivi => demander le consentement <p>Demander le consentement pour les fonctionnalités venant d'autres sites (Google, Facebook...)</p>	<p>https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs</p> <p>https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite</p> <p>https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-maitriser-votre-navigateur</p> <p>Approfondir :</p> <p>https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles</p> <p>https://www.cnil.fr/sites/default/files/atoms/files/projet_de_recommandation_cookies_et_autres_traceurs.pdf</p>

