Imperiatus
./L'agence_digitale

CHECKLIST RGPD POUR LES ENTREPRISES
GUIDE DE CONFORMITÉ

Cette checklist vous permet de vérifier dans les grandes lignes la conformité de votre entreprise au Règlement Général sur la Protection des Données (RGPD). Elle s'applique à toutes les entreprises qui traitent des données personnelles de résidents européens, quelle que soit leur taille.

Certains des points sont obligatoires pour toutes les entreprises, certaines ne sont obligatoires que selon vos usages des données et d'autres encore sont des recommandations pertinentes à mettre en place.

Note : Imperiatus (EI Pierre DARME) fourni cette liste qui ne peut pas être considérée comme exhaustive : le sujet de la protection des données est un sujet complexe qui nécessite une analyse approfondie dont aucune méthode universelle ne peut être appliquée.

PRÉALABLES ET DIAGNOSTIC

Définition des données personnelles

J'ai identifié ce qui constitue une donnée personnelle dans mon entreprise
Je comprends la différence entre données personnelles et données anonymisées
J'ai identifié les traitements de données personnelles effectuées dans mon entreprise.

Applicabilité du RGPD

Mon entreprise traite des données de résidents européens
Mon entreprise est établie dans l'UE ou cible des résidents européens
J'ai vérifié si mon entreprise agit comme responsable de traitement ou sous-traitant

GOUVERNANCE ET ORGANISATION

Délégué à la Protection des Données (DPO)

J'ai vérifié si la désignation d'un DPO est obligatoire pour mon entreprise :

- Autorité/organisme public
- Traitement à grande échelle de données sensibles
- Surveillance systématique à grande échelle

Si obligatoire : j'ai désigné un DPO et déclaré sa désignation à la CNIL
Si non obligatoire : j'ai évalué l'opportunité de désigner un DPO volontairement
Le DPO dispose des compétences, moyens et indépendance nécessaire
Le DPO est impliqué dans toutes les questions relatives à la protection des données

Responsabilités internes

J'ai désigné un pilote interne pour la conformité RGPD
Les rôles et responsabilités sont définis et documentés
La direction est impliquée dans la démarche de conformité
Un budget est alloué à la mise en conformité

REGISTRE DES TRAITEMENTS

Création du registre

J'ai créé un registre des activités de traitement (obligatoire)
Le registre est tenu sous forme écrite (papier ou électronique)
Je distingue le registre «responsable de traitement» du registre «sous-traitant» si applicable

Contenu du registre (pour chaque traitement)

Nom et coordonnées du responsable de traitement
Nom et coordonnées du DPO (si applicable)
Finalités du traitement (objectif poursuivi)
Catégories de personnes concernées (clients, employés, prospects, etc.)
Catégories de données personnelles traitées
Catégories de destinataires (qui accède aux données)
Durée de conservation des données
Description des mesures de sécurité mises en place
Transferts hors UE (si applicable) et garanties associées

Maintenance du registre

Le registre est régulièrement mis à jour
Chaque nouveau traitement est ajouté au registre
Les traitements supprimés sont retirés du registre
Le registre est accessible pour contrôle CNIL

BASES LÉGALES ET FINALITÉS

Identification des bases légales

Pour chaque traitement, j'ai identifié la base légale :

- Consentement de la personne
- Exécution d'un contrat
- Obligation légale
- Sauvegarde des intérêts vitaux
- Mission d'intérêt public
- Intérêt légitime (avec test de proportionnalité)

Finalité des traitements

Chaque traitement a une finalité déterminée, explicite et légitime
Les données ne sont pas utilisées pour d'autres finalités incompatibles
Les nouvelles finalités font l'objet d'une analyse de compatibilité

PRINCIPES FONDAMENTAUX

Minimisation des données

Je ne collecte que les données strictement nécessaires
J'ai supprimé les données inutiles ou excessives
Les formulaires ne demandent que les informations indispensables

Exactitude des données

J'ai mis en place des procédures pour maintenir les données à jour
Les données inexactes sont corrigées ou supprimées
Les personnes peuvent facilement corriger leurs données

Limitation de la conservation

J'ai défini des durées de conservation pour chaque catégorie de données
Les durées sont justifiées et documentées
J'ai mis en place des procédures d'effacement automatique ou manuelle
Les données en archive sont clairement identifiées

Procédures d’exercice des droits

J’ai mis en place des procédures pour traiter les demandes d’exercice de droits :

- Droit d’accès
- Droit de rectification
- Droit à l’effacement (droit à l’oubli)
- Droit à la limitation du traitement
- Droit à la portabilité
- Droit d’opposition

Les procédures permettent de répondre dans un délai d’un mois
Des formulaires ou canaux dédiés facilitent l’exercice des droits
Les demandes sont authentifiées et tracées

Consentement (si applicable)

Le consentement est libre, spécifique, éclairé et univoque
Le consentement est recueilli par un acte positif (pas de cases pré-cochées)
Je peux prouver que le consentement a été donné
Les personnes peuvent retirer facilement leur consentement
Le retrait du consentement est aussi simple que son obtention

SÉCURITÉ DES DONNÉES

Mesures techniques de sécurité

Authentification forte et gestion des accès
Chiffrement des données sensibles
Pseudonymisation des données quand cela est possible
Sauvegarde régulières et testées
Antivirus et protection contre les malwares
Pare-feu et segmentation réseau
Mise à jour régulière des systèmes
Journalisation des accès et activités

Mesures organisationnelles de sécurité

Politique de sécurité documentée et communiquée
Formation du personnel à la sécurité des données
Contrôle des accès physiques aux locaux
Clauses de confidentialité dans les contrats de travail
Procédures de travail sécurisées
Plan de continuité et de reprise d’activité
Tests réguliers des mesures de sécurité

Évaluation des risques

J’ai identifié les risques pesant sur les données personnelles
Les mesures de sécurité sont proportionnées aux risques
L’évaluation des risques est régulièrement mise à jour

VIOLATION DE DONNÉES

Procédure de gestion des incidents

J’ai défini des procédures de détection des violations de données
J’ai identifié les personnes à contacter en cas d’incident
J’ai préparé les modèles de notification à la CNIL
J’ai défini les critères de notification aux personnes concernées

Documentation des violations

Toute violation est documentée en interne (nature, conséquences, mesures)
Un registre des violations est tenu
Les violations susceptibles de créer un risque sont notifiées à la CNIL sous 72h
Les violations à risque élevé sont notifiées aux personnes concernées

TRANSFERTS INTERNATIONAUX

Identification des transferts

J’ai identifié tous les transferts de données hors UE/EEE
Je distingue les vrais transferts des simples accès depuis l’étranger

Encadrement des transferts

Pour les pays avec décisions d’adéquation : transfert libre
Pour les autres pays, j’utilise un outil d’encadrement :

- Clauses contractuelles types
- Règles d’entreprise contraignantes (BCR)
- Codes de conduite ou certifications
- Dérogations de l’article 49 du RPGD (exceptionnellement)

J’ai effectué une analyse d’impact pour les transferts (AITD)

Contrats de sous-traitance

Tous les contrats incluent les clauses RGPD obligatoires :

- Objet, durée, nature et finalité du traitement
- Catégories de données et de personnes concernées
- Obligations du sous-traitant
- Assistance pour les droits des personnes
- Assistance pour la sécurité et les violations
- Conditions des transferts internationaux
- Retour ou destruction des données en fin de contrat

Les contrats sont signés avant le début des traitements

COOKIES ET TRACEURS

Audit des cookies

J’ai recensé tous les cookies et traceurs sur mon site web
J’ai classé les cookies par catégorie (nécessaires, fonctionnels, analytiques, publicitaire)

J’ai identifié la finalité de chaque cookie

Gestion du consentement

Une bannière de consentement est présente sur le site
Le consentement est demandé avant le dépôt des cookies (sauf cookies nécessaires)

Les utilisateurs peuvent accepter/refuser par catégorie
Les utilisateurs peuvent modifier leur consentement à tout moment
Le consentement est enregistré et horodaté

Information sur les cookies

Une politique de cookies détaillée est accessible
La politique liste tous les cookies et leurs finalités
Les coordonnées pour exercer ses droits sont indiquées

ANALYSE D'IMPACT (AIPD/DPIA)

Identification des traitements à risque élevé

J'ai identifié les traitements nécessitant une AIPD :

- Évaluation/notation systématique à grande échelle
- Traitement à grande échelle de données sensibles
- Surveillance systématique à grande échelle
- Traitements figurant sur la liste CNIL

Les nouveaux traitements sont évalués systématiquement

Réalisation des AIPD

Les AIPD sont réalisées avant la mise en œuvre des traitements
Les AIPD comprennent :

- Description du traitement
- Évaluation de la nécessité et proportionnalité
- Évaluation des risques pour les personnes
- Mesures pour traiter les risques

Le DPO est consulté (si applicable)
Les AIPD sont mises à jour en cas de modification

DOCUMENTATION ET FORMATION

Documentation de la conformité

Toutes les analyses et décisions sont documentées
Les procédures internes sont formalisées
La documentation est régulièrement mise à jour
Les preuves de conformité sont conservées

Formation et sensibilisation

Les équipes sont formées au RGPD
Des sessions de sensibilisation régulières sont organisées
Les nouveaux collaborateurs reçoivent une formation RGPD
Des guides pratiques sont mis à disposition

VEILLE ET CONFORMITÉ CONTINUE

Suivi de la réglementation

Je maintiens une veille sur l'évolution du RGPD et des recommandations CNIL
Je suis les décisions de justice et sanctions
J'adapte mes pratiques aux nouvelles recommandations

Contrôles internes

J'effectue des audits internes réguliers
Je teste régulièrement mes procédures
Je corrige rapidement les non-conformités identifiées

Préparation aux contrôles CNIL

Je suis prêt à recevoir un contrôle CNIL
La documentation est organisée et accessible
Les équipes savent comment réagir en cas de contrôle

FAITES VOUS ACCOMPAGNER

Pierre DARME
Consultant web et délégué à la protection des données

Contact@imperiatus.com
www.imperiatus.com

ATTENTION - SANCTIONS POSSIBLES

Le non-respect du RGPD peut entraîner :

- **Amendes administratives :** jusqu'à 20 millions d'euros ou 4% du CA annuel mondial
- **Sanctions pénales** selon la législation nationale
- **Atteinte à la réputation** et perte de confiance des clients
- **Interruption d'activité** en cas d'injonction

PLANNING DE MISE EN CONFORMITÉ

- **Phase 1 (mois 1-2) :** diagnostic et registre des traitements
- **Phase 2 (mois 2-3) :** mise en place des procédures droits des personnes
- **Phase 3 (mois 3-4) :** sécurisation des données et formation du personnel
- **Phase 4 (mois 4-6) :** finalisation et contrôles internes