GUIDE DE MISE EN CONFORMITE RGPD


cgpi
consulting

AVANT-PROPOS

Le RGPD est une étape majeure dans la protection des données. Il vise à renforcer l'importance de cet enjeu auprès de ceux qui traitent les données et à responsabiliser les professionnels. Il consacre et renforce les grands principes de la loi Informatique et Libertés, en vigueur depuis 1978, et accroît sensiblement les droits des citoyens en leur donnant plus de maitrise sur leurs données.

A partir du 25 Mai 2018 toutes les entreprises devront avoir entamé une démarche de mise en conformité avec le RGPD. Les modalités de contrôle resteront les mêmes qu'auparavant mais les sanctions prévues par ce nouveau règlement sont fortement dissuasives.

La sécurité n'est plus une option. À ce titre, les enjeux de sécurité numérique doivent se rapprocher des préoccupations économiques, stratégiques ou encore d'image qui sont celles des décideurs. Ce document a pour objectif de vous donner les bases pour entamer une démarche de mise en conformité. Nous pouvons vous proposer un accompagnement mais nous sommes convaincus que la démarche de protection des données doit être ancrée dans vos processus et venir d'une décision stratégique forte de votre entreprise.

SOMMAIRE

– ANALYSER LES RISQUES : LE REGISTRE DES TRAITEMENTS

La rédaction du registre des traitements est une obligation pour les entreprises de plus de 250 employés. Ce registre peut être consulté à tout moment par la CNIL et doit comporter des informations sur le responsable du traitement, les destinataires des données et la finalité du traitement (profilage, analyse statistique, conception d'offres commerciales…).

Pour les autres entreprises même s'il n'existe pas d'obligation, nous vous conseillons fortement la création d'un tel document qui ne pourra que renforcer vos chances de succès en cas de contrôle. D'autant plus qu'il est obligatoire de procéder à l'évaluation des risques impliquant des données à caractère personnel. Pour chaque traitement vous devez répondre aux questions suivantes et consigner les réponses dans un document.

On entend par traitement le fait d'utiliser des données dans le cadre de son activité. Par exemple : Facturation client, Analyse des ventes, Prospection commerciale, Obligation règlementaire…

Pour chaque traitement il convient de créer une fiche qui se compose de trois parties.

La tenue de ce registre peut se faire à l'aide du fichier Excel nommé « Registre-des-traitements » qui est proposé comme modèle par la CNIL ou encore à l'aide du logiciel PIA disponible en téléchargement depuis le site la CNIL.

Partie 1 : Contexte

Quel est le traitement qui fait l'objet de l'étude ?
Présentez le traitement de manière synthétique (Nom, finalité, enjeux)

Quelles sont les responsabilités liées au traitement ?
Indiquez l'identité du responsable, les sous-traitants impliqués et les autres responsables

Quelles sont les données traitées ?
Listez les données collectées, les durées de conservation et les personnes pouvant y accéder

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?
Décrivez le processus du traitement des données. Depuis la collecte à la destruction ou l'archivage

Quels sont les supports des données ?
Listez les supports utilisés (Logiciels, serveurs, papier, …)

Partie 2 : Principes fondamentaux

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?
Expliquez en quoi les données que vous récoltez sont légitimes et pertinentes pour votre activité

Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?
Présentez le cadre d'utilisation du traitement des données (contrat, obligation réglementaire, …)

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?
Expliquez en quoi les données que vous collectez sont nécessaire pour le traitement

Les données sont-elles exactes et tenues à jour ?
Indiquez quelles mesures sont prévues pour conserver ces données à jour

Quelle est la durée de conservation des données ?
Indiquez en quoi durée de conservation prévue pour ces données est nécessaire à la finalité de votre traitement

Comment les personnes concernées sont-elles informées à propos du traitement ?
Indiquez les moyens mis en place pour informer les clients que leurs données sont protégées

Comment le consentement des personnes est-il obtenu ?
Indiquez comment vous avez recueillis les données à caractère personnel

Comment les personnes concernées peuvent-elles exercer leur droit d'accès et droit à la portabilité ?
Indiquez comment les personnes concernées peuvent accéder à leurs données pour les modifier et les transmettre

Comment les personnes concernées peuvent-elles exercer leur droit de rectification et droit à l'effacement (droit à l'oubli) ?
Indiquez comment les personnes concernées peuvent supprimer leurs données

Partie 3 : Risques

Quelles sont les mesures existantes ou prévues ?

Pour chaque traitement il faut répondre aux questions suivantes à chaque fois dans les cas d'accès illégitimes à des données, de modification non désirée de données ou de disparition de données.

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Quelles sources de risques pourraient-elles en être à l'origine ?

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

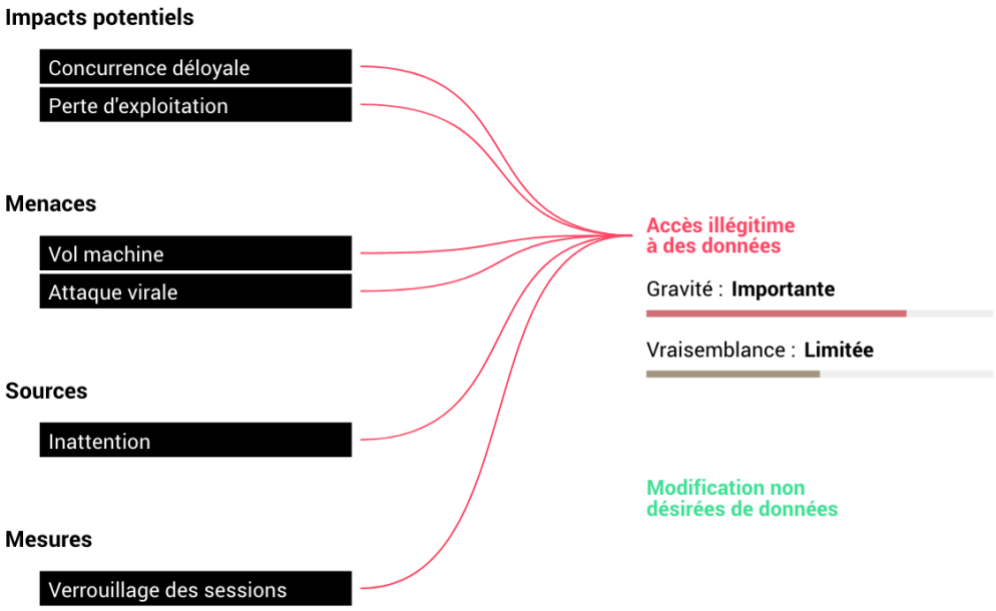
- Négligeable

- Limitée
- Importante
- Maximale

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

- Négligeable
- Limitée
- Importante
- Maximale

L'objectif de ce processus est de créer une cartographie des risques sous



Ci-dessous une liste de mesures à mettre en place en fonction du risque.

<u>Risque d'intrusion</u>

#	Mesure	Standard	Renforcé
1	Mettre en place un firewall et un antivirus sur chaque poste	X	
2	Mettre en place une gestion des droits d'accès aux données (Se poser la question : Est-ce que l'utilisateur x a besoin d'accéder aux données de M. ou Mme Y ?)	X	
3	Mettre en place une politique de gestion des mots de passe	X	
4	Mettre en place des accords de non divulgation des informations avec les prestataires ayant accès aux données personnelles	X	
5	Prévenir les personnes concernées en cas d'intrusion aux données	X	
6	Sensibiliser les utilisateurs à faire attention à la confidentialité des données	X	

7	Restreindre les accès aux locaux par des portes verrouillées	X	
8	Installer des alarmes anti-intrusion et vérifiez-les régulièrement		X
9	Utiliser des algorithmes de cryptage pour les supports amovibles et les ordinateurs portables	X	
10	Installer les dernières mises à jour de sécurité des systèmes d'exploitation	X	
11	Verrouiller automatiquement les sessions des ordinateurs après un délai d'inactivité	X	
12	Mettre en place le protocole WPA pour les clés des réseaux Wifi	X	
13	Chiffrez les données personnelles avant leur envoi		X
14	Ne transmettez jamais les identifiants et les mots de passe dans le même envoi et si possible faites le par deux canaux différents		X
15	Créer un réseau wifi dédié aux personnes extérieures à votre organisation et conserver les logs d'accès	X	
16	Mettre en place une authentification à deux facteurs pour la consultation des données sensibles		X
17	Mettre en place sur le réseau un firewall avec des règles de restriction d'accès strictes		X
18	N'installez pas d'applications non autorisées par votre service informatique		X

Risque de modification non désirée des données

#	Mesure	Standard	Renforcé
1	S'assurer que chaque utilisateur dispose d'un identifiant unique pour accéder aux données	X	
2	Anonymiser les données		X
3	Mettre en place un système de journalisation	X	
4	Limitez les flux réseau au strict nécessaire		X
5	Ne plus utiliser les logiciels dont le support est interrompu	X	

Risque de perte des données

#	Mesure	Standard	Renforcé
1	Mettre en place un plan de sauvegarde pertinent	X	
2	Prévoir des tests de continuité d'activité au moins tous les semestres		X
3	Faire régulièrement des vérifications sur l'intégrité de la sauvegarde	X	

4	S'assurer que les salariés sont formés à la récupération des données en cas de perte		X

II – METTRE EN PLACE UNE POLITIQUE DES MOTS DE PASSE

A minima, l'ANSSI estime que les 8 recommandations suivantes doivent s'appliquer indépendamment de tout contexte. Lorsque les systèmes d'information utilisés le permettent, certaines doivent être imposées techniquement.

R1 : Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts.

R2 : Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).

R3 : Ne demandez jamais à un tiers de créer pour vous un mot de passe.

R4 : Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.

R5 : Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.

R6 : Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.

R7 : Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.

R8 : Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

Pour créer un mot de passe sécurisé vous pouvez utiliser l'une des deux méthodes suivantes :

Méthode phonétique : Cette méthode consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple la phrase « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am.

Méthode des premières lettres : Cette méthode consiste à garder les premières lettres d'une phrase (citation, paroles de chanson…) en veillant à ne pas utiliser que des minuscules. Par exemple, la citation « un tiens vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

Les mots de passe doivent avoir une date de validité maximale. A partir de cette date l'utilisateur ne doit plus pouvoir s'authentifier sur le système si le mot de passe n'a pas été changé. Ceci permet de s'assurer qu'un mot de passe découvert par un utilisateur mal intentionné, ne sera pas utilisable indéfiniment dans le temps.

Pour aller plus loin

L'utilisation d'un logiciel de gestion des mots de passe est recommandée. Ces logiciels vous permettent de garantir que les mots de passe sont à jour, de changer facilement les mots de passe en cas de départ d'un collaborateur et d'avoir des mots de passe forts. Nous vous recommandons les logiciels **Dashlane** et **Lastpass**.

III – LE RESPECT DES DROITS DES UTILISATEURS

C'est ici très certainement le point le plus important à respecter. Vous devez recueillir et conserver une preuve du consentement de chaque utilisateur pour l'utilisation de ses données personnelles. Vous devrez par la même occasion préciser à l'utilisateur dans quel contexte ses données seront utilisées.

Les utilisateurs pourront également exercer leur droit à l'oubli (Effacement de ses données) et le droit à la portabilité de leurs données (transmission à un organisme tiers).

Prévoyez donc d'intégrer dans tous vos documents demandant des informations personnelles une case à cocher indiquant clairement que les données pourront être utilisées et dans quel cadre.

Important : L'utilisation des adresse email pour des communications autres que celles qui rentrent dans le cadre normal de la relation client-fournisseur, doit faire l'objet d'un consentement spécial. Par exemple vous ne pouvez pas utiliser les adresses de vos clients pour communiquer sur un nouveau produit si vous n'avez pas préciser ce cas dans le consentement initial.

Le cryptage des données

Le cryptage et l'anonymisation des données est une obligation uniquement pour les données sensibles. Le cadre des données sensibles a été mis à jour et continent désormais les éléments suivants :

- ➔ Origines raciales
- ➔ Opinions politiques ou religieuses
- ➔ Orientation sexuelle
- ➔ Données biométriques et/ou génétiques
- ➔ Toute autre information liée à la santé

Toutefois la CNIL recommande d'utiliser le chiffrement pour tous les supports mobile (disque dur externe, ordinateurs portable, clés USB) car ceux-ci sont plus exposés aux risques de vols que les matériels fixes.

Pour chiffrer un disque dur vous pouvez utiliser les logiciels **BitLocker** ou **VeraCrypt**.

Pour aller plus loin

Nous vous recommandons également de chiffrer vos fichiers lors de vos envois de fichiers sensibles à vos clients ou partenaires (extraits de compte, documents d'identité, …). Pour ce faire nous vous recommandons l'utilisation des logiciels **AxCrypt** ou **7-zip** qui vont vous permettre de créer une archive protégée par mot de passe. Pour garantir une sécurité optimale nous vous encourageons à communiquer le mot de passe par SMS ou par téléphone.

IV – ACTUALISER LES CONTRATS FOURNISSEURS

Dans le cadre de la RGPD vous devez vous assurer que les fournisseurs et les sous-traitants avec lesquels vous travaillez ont eux-mêmes entamés un processus de mise en conformité.

Dans le cas où vous avez un contrat avec ceux-ci, pensez à rajouter une clause stipulant que votre relation de travail devra être en conformité avec la RGPD. Dans la mesure du possible faites un avenant pour formaliser cette démarche.

Pour aller plus loin

Prévoyez une clause de confidentialité dans vos contrats de sous-traitance
Enregistrer les différentes interventions des sous-traitants dans un registre
Effacez toutes les données des ordinateurs avant de les recycler
Assurer-vous d'avoir un matériel sous garantie
Veillez à ce que les sous-traitants n'accèdent pas à vos postes de travail sans votre autorisation

V – ELABORER UNE CHARTE INFORMATIQUE

Afin de sensibiliser vos équipes à l'importance de la protection des données il est utile de rédiger une charte d'utilisation des outils informatiques que vous pourrez annexer au règlement intérieur.

D'une manière générale il est important de sensibiliser les utilisateurs à la protection des données comme éviter les copies de fichiers sur des supports non autorisés, d'éviter d'installer des outils non validés par le service informatique ou encore de noter les mots de passe sur des documents papier.

Pour aller plus loin

La CNIL fournit un exemple de charte informatique qu'il vous conviendra de personnaliser en fonction de votre activité. Vous trouverez ce modèle en annexe ou via ce lien.

VI – ELABORER UN PLAN D'ACTION ET VALIDER SA DEMARCHE

C'est là une obligation introduite par la RGPD, en cas d'incident pouvant avoir un impact sur les données personnelles vous avez l'obligation de mettre en place un plan d'action. Ce plan d'action peut varier en fonction de la nature de l'incident.

Pour vous aider
Voici ci-dessous un exemple de procédure en cas de détection d'intrusion (piratage).

1. Déconnecter les postes infectés du réseau
2. Prévenir le DPD responsable du ou des traitements concernés
3. Identifier l'origine de la faille de sécurité ayant permis l'intrusion
4. Corriger la faille de sécurité
5. Vérifier l'intégrité des données (modifications non désirées ou pertes)
6. Alerter les personnes potentiellement concernées par l'incident

Pour plus d'efficacité vous pouvez compléter ce document avec les coordonnées directes des contacts ou les logiciels à utiliser.

Faire valider sa démarche

Une fois la démarche terminée le DPD, les personnes concernées par le traitement et le responsable des traitements doivent donner un avis sur les mesures en place. Le document d'analyse d'impact peut alors être validé, à améliorer (fixez-vous des échéances) ou refusé.
Le DPD peut également valider seul le document, il doit alors justifier le fait d'être passé outre l'avis des autres personnes concernées.

VII – MA CHECKLIST

Mon plan RGPD en 5 jours

Jour 1 – Je désigne un responsable RGPD et je relis le guide

Prévoir environ 1h.

Jour 2 – Je commence mon registre des traitements

A l'aide du logiciel PIA ou sur un nouveau document, je fais la liste des traitements de mon entreprise. Prévoir environ 1h30.

Jour 3 – J'évalue les risques

Pour chaque traitement je détermine quels sont les risques et je choisis en même temps les mesures à mettre en place. Je fais la cartographie des risques. Prévoir environ 1h30.

Jour 4 – Je créé ma charte informatique et j'actualise mes documents

Je complète le document modèle de charte informatique. Je contacte mes fournisseurs pour mettre à jour les contrats. Je mentionne la RGPD et j'ajoute une phrase de consentement dans les documents à destination de mes clients. Prévoir environ 2h30.

Jour 5 – Je créé mon plan d'action et je valide ma démarche

Je fais la liste des mesures à prévoir et je les planifie. Prévoir environ 1h00.

BIBLIOGRAPHIE

Guides des bonnes pratiques de mot de passe
https://www.ssi.gouv.fr/guide/mot-de-passe/