
IKIGAI


cci
NOUVELLE-CALÉDONIE

Informations

L'Etat français a confié à **Bpifrance** (**avec France Num dans le cadre du Plan de relance**), l'organisation d'un programme de sensibilisation au numérique pour les **TPE/PME**. Bpifrance a par la suite organisé un appel à projet afin de trouver localement des organismes pouvant assurer cette sensibilisation au travers d'ateliers. Sur le territoire, c'est **OPEN NC** a remporté cet appel à projet et organise donc des ateliers de sensibilisation à la transformation numérique 100% gratuits. Aujourd'hui, en partenariat avec Cap Digital.

Bon atelier !

Financé par GOUVERNEMENT Liberté Égalité Fraternité — FRANCE RELANCE — Union européenne NextGenerationEU

À l'initiative de [N] FRANCE NUM

bpifrance

OPEN NOUVELLE-CALEDONIE ORGANISATION DES PROFESSIONNELS DE L'ECONOMIE NUMÉRIQUE

setup

cci NOUVELLE-CALÉDONIE

Quelle démarche pour se simplifier la vie face au RGPD ?

Stephane Deck d'Ikigai

IKIGAI

CCI NOUVELLE-CALÉDONIE

CAP DIGITAL

Entreprises, prenez
le virage du numérique,
la CCI vous accompagne

L'accompagnement individuel au cœur du dispositif

- **Diagnostic numérique** approfondi avec votre conseiller CCI
- **Plan d'actions priorisé** et suivi personnalisé
- **RDV conseil thématique** sur une problématique spécifique

Des matinales et des ateliers pratiques

- Animés par des **professionnels** du numérique
- En partenariat avec **OPEN-NC** et l'**Observatoire du Numérique NC**

IKIGAI

cci NOUVELLE-CALÉDONIE

Sommaire

IKIGAI

cci NOUVELLE-CALÉDONIE

Présentation de votre intervenant

Stéphane DECK

IKIGAI 生き甲斐 : mot japonais qui désigne le sens que l'on donne à sa vie.

IKIGAI est une entreprise d'accompagnement dans vos projets et audits. Née d'une vision de la qualité et de la cybersécurité, nous collaborons avec de nombreux acteurs nationaux afin d'assurer un périmètre global de couverture des problématiques

1.

Principes du RGPD

Principes du RGPD

Voila ce que le RGPD a apporté à la règlementation alors en vigueur (Loi Informatique et Liberté).

RGPD	Harmonisation des législations européennes en matière de protection des données avec une application directe (sans transposition)
	Changement de paradigme avec un passage d'un régime de déclaration et d'autorisation préalable à l'accountability (responsabilisation du responsable de traitement)
	Renforcement des droits des personnes pour leur donner plus de maitrise sur leurs données
	Création de la fonction de DPO, véritable chef d'orchestre de la protection des données
	Approche de la protection des données par le risque afin de minimiser les impacts sur la vie privée des personnes
	L'obligation de mettre en place des mesures de sécurité adéquates pour garantir la confidentialité des données
	Répartition des responsabilités entre responsables de traitement et sous-traitants
	Renforcement des sanctions de la CNIL

2.

Quelques définitions

Principes du RGPD

Quelques définitions – donnée personnelle

- Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable.

<u>Une personne physique peut être identifiée :</u>

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de DN, une adresse postale ou courriel, mais aussi la voix ou l'image).

<u>L'identification d'une personne physique peut être réalisée :</u>

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).

Quelques définitions

Quelques définitions – donnée sensible

Les données sensibles forment une catégorie particulière des données personnelles.

Ce sont des informations qui révèlent :

- la prétendue origine raciale ou ethnique,
- les opinions politiques,
- les convictions religieuses ou philosophiques ou l'appartenance syndicale,

ou qui traitent :

- des données génétiques,
- des données biométriques aux fins d'identifier une personne physique de manière unique,
- des données concernant la santé,
- des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

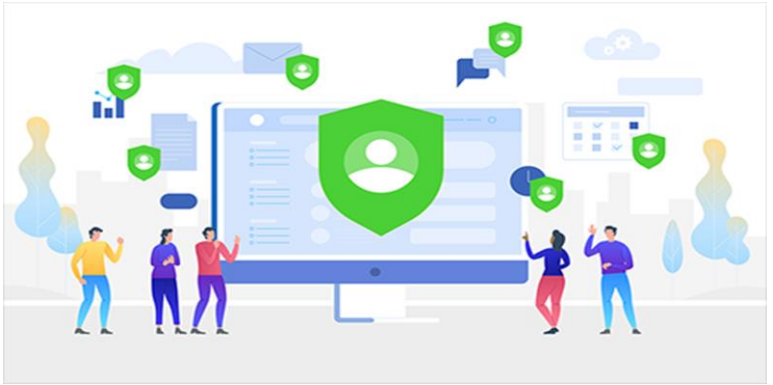
Quelques définitions

Quelques définitions – traitement de données personnelles

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

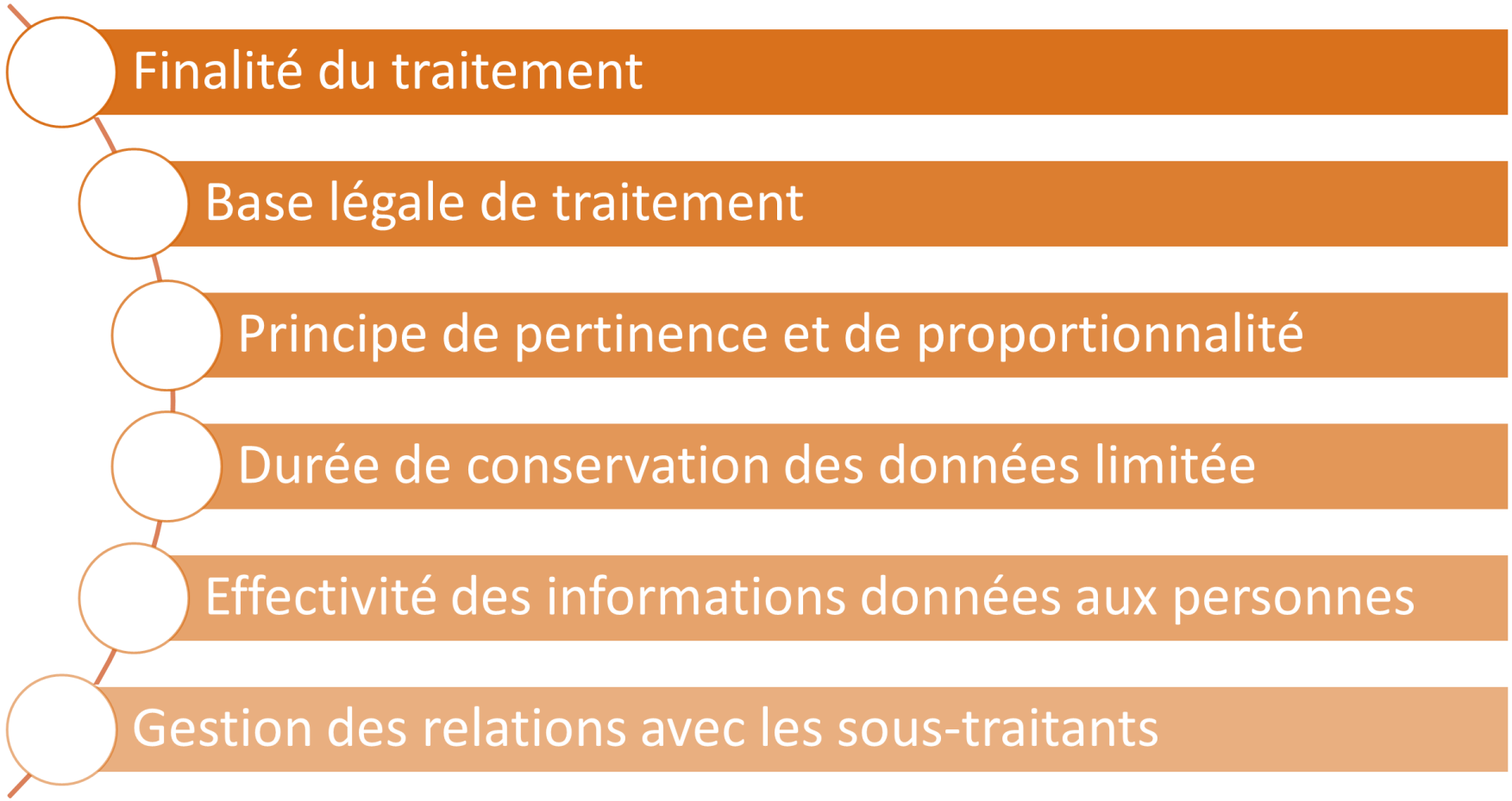
Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation.



3.

Principes à respecter

Principes à respecter pour les traitements des données personnelles



4.

Droits des personnes

Principes à respecter pour les traitements des données personnelles

- Toute personne a le droit d'accéder aux données qui la concernent et qui font l'objet d'un traitement.

Droit d'accès

- Toute personne peut demander la rectification des informations inexactes la concernant. Ce droit permet d'éviter le traitement ou la diffusion de fausses informations.

Droit de rectification

- Les personnes peuvent demander à un organisme l'effacement des données personnelles les concernant

Droit d'effacement

- Toute personne a le droit de demander à un organisme de geler temporairement l'utilisation de certaines de ses données

Droit à la limitation du traitement

- Toute personne a la possibilité de transférer ses données d'un système d'information à un autre

Droit à la portabilité

- Toute personne a le droit de s'opposer à ce que ses données fassent l'objet d'un traitement.

Droit d'opposition

IKIGAI

cci NOUVELLE-CALÉDONIE

5.

Risques en cas de non-conformité

Risques en cas de non-conformité

Risque financier

Certains manquements relatifs aux obligations de formalisme et à la sécurité des données sont sanctionnés dans un maximum de 10 millions d'euros ou 2 % du chiffre d'affaires mondial.

Des actions de groupe peuvent être menées aux fins d’indemnisation des préjudices subis par les personnes concernées, des dommages et intérêts , enfin, des amendes pénales peuvent également être prononcées

Risques en cas de non-conformité

Risque d’exploitation

Le non-respect des règles peut entrainer une interdiction administrative de la mise en oeuvre des traitements de données à caractère personnel considérés illicites ce qui peut conduire à suspendre l’activité de l’entreprise qui repose sur ces traitements.

Parfois, la simple demande de mise en conformité d'une entreprise peut entrainer une extinction de l'activité de l'entreprise.

Par ailleurs, à la suite d'un vol ou d'une perte de données, l’activité de l’entreprise peut être suspendue voire anéantie.

Risques en cas de non-conformité

Risque commercial

Le RGPD est à destination des organisations, des entreprises, des collectivités et du marché. Il assure la libre circulation des données. Ainsi, les acteurs économiques doivent respecter ses règles pour travailler avec des données personnelles.

Une absence de conformité au RGPD peut entraîner une perte de marché ou une perte de contrat dans le cadre d'un appel d'offres par exemple. En effet, des obligations spécifiques existent à destinatation des sous-traitants. Un sous-traitant qui ne présenterait pas de garanties de conformité au RGPD (notamment dans son contrat par exemple) pourrait se voir refuser un marché au profit d'un autre plus vertueux.

Risques en cas de non-conformité

Risque d'image

C'est probablement le risque le plus important, Le RGPD est un corpus de règles à destination des organisations conçu pour rééquilibrer leur rapport de force avec les personnes concernées dans la mise en œuvre des traitements.

Un manquement aux règles essentielles peut être facilement vécu comme une trahison et générer de la perte de confiance.

Par ailleurs, n'oublions pas que les sanctions et mises en demeure de la CNIL peuvent être rendues publiques.

Risques en cas de non-conformité

Risque juridique

Les traitements de donnés personnelles servent pour beaucoup à titre de preuve dans des contentieux en droit social ou commercial.

Risques en cas de non-conformité

Risque pénal

Les manquements aux règles de protection des données font pratiquement tous l'objet de sanctions pénales pouvant aller jusqu'à **5 ans de prison et 300 000 euros** d'amende pour les dirigeants et **1 500 000 euros d'amende pour la personne morale**.

Risques en cas de non-conformité

Risque de non-conformité

Une **plainte ou demande d'exercice d'un droit d’un sala rié ou d’un client** mal gérée peut générer des alertes auprès des autorités de contrôle et contraindre l'organisation dans un **processus de contrôle**.

6.

Les questions à se poser et les principes à respecter

Les questions à se poser et les principes à respecter

Finalité du traitement

- Quel est l’objectif final de mon traitement?
- Comment puis-je le formuler pour qu’il soit explicite?

Les questions à se poser et les principes à respecter

Base légale de traitement

- Est-il possible de réaliser ce traitement sur une base contractuelle?
- Dois-je demander un consentement? Si oui comment puis le conserver? Devrais-je gérer des consentements à nouveau?
- L'intérêt légitime peut-il être mis en place?

Les questions à se poser et les principes à respecter

Principe de pertinence et de proportionnalité

- Quelles données je récupère dans mon traitement?
- Ai-je des données sensibles?
- Ai-je besoin de toutes ces données?
- Sont-elles pertinentes en regard de ma finalité?
- Quels impacts réels si j'en réduit le périmètre?

Les questions à se poser et les principes à respecter

Durée de conservation des données limitée

- Pourquoi je conserve les données aujourd'hui?
- Quels sont réellement les usages que j'en fait? Les 3 dernières années? Cette année?
- Comment sont-elles conservées et quels sont mes coûts réels de conservation?
- Quelle durée légitime et règlementaire sur mon traitement?

Les questions à se poser et les principes à respecter

Effectivité des informations données aux personnes

- Ai-je informé les personnes concernées sur ce traitement?
- Comment les ai-je informées et puis-je le prouver?
- Les personnes concernées savent-elles comment revenir vers moi concernant ce traitement?

Les questions à se poser et les principes à respecter

Gestion des relations avec les sous-traitants

- Me suis-je bien protégé contractuellement avec mes fournisseurs et prestataires?
- Ont-ils accès aux données dont je suis responsable? Si oui en ont-ils besoin? Pour quelles finalités?
- Comment mon sous-traitant assure t'il la protection des données dont je suis responsable?

7.

Corpus documentaire

Corpus documentaire

Des éléments de documentation à produire

LA DOCUMENTATION SUR VOS TRAITEMENTS DE DONNÉES PERSONNELLES

- **Le registre des traitements** (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants)
- **Les analyses d'impact relatives à la protection des données** (AIPD) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes

L'INFORMATION DES PERSONNES

- **Les mentions d'information**
- Les modèles de **recueil du consentement des personnes concernées**,
- Les procédures mises en place pour **l'exercice des droits**

LES CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS

- **Les contrats avec les sous-traitants**
- Les procédures internes **en cas de violations de données**
- Les preuves que les personnes concernées **ont donné leur consentement** lorsque le traitement de leurs données repose sur cette base.

Corpus documentaire

Quelques références

Professionnel | CNIL

Le registre des activités de traitement | CNIL

Entreprises : comment mettre en œuvre les droits des utilisateurs conformément au RGPD ? - francenum.gouv.fr

Êtes-vous « RGPD friendly » ? - francenum.gouv.fr

Autodiagnostic RGPD : votre TPE-PME est-elle en conformité ? - francenum.gouv.fr

8.

Comment se simplifier la vie face au RGPD

Comment se simplifier la vie face au RGPD

Connaitre le RGPD

Faites un diagnostic

Evaluez votre risque

Soyez pragmatiques

Acceptez que ce sera peut-être long

Profitez-en pour améliorer l'existant

IKIGAI

cci NOUVELLE-CALÉDONIE

MERCI DE VOTRE ATTENTION

IKIGAI

OPEN
NOUVELLE-CALEDONIE
ORGANISATION DES PROFESSIONNELS DE L'ECONOMIE NUMÉRIQUE

CCI
NOUVELLE-CALÉDONIE