CYBER FOR GOOD

assoconnect

RGPD et associations 🔒

(21.03.2024)

Objectif

Décomplexifier les (nouvelles) règlementations “cyber”

Qui sommes-nous ?

Antoine Ortiz
-
AssoConnect
-
Responsable contenu

Cyrille Chauvel
-
Advens
-
Consultant Cyber Conformité pour Cyber for Good

Belkacem Massyl
-
Devoteam
-
Consultant Cyber security pour Cyber for Good

Charlotte Flesch
-
Latitudes
-
Responsable du programme Cyber for Good

Cyber for Good, c’est quoi ?

Le premier programme complet de sensibilisation, d'acculturation et d'accompagnement pro bono sur les enjeux cyber pour les acteurs de l'ESS.

1

Webinaires de sensibilisation

aux enjeux et risques de la cybersécurité pour l’ESS

2

Rencontres d’1h

avec des spécialistes en cyber pour répondre à toutes vos questions

3

Accompagnement long

sur mesure si vous avez des besoins spécifiques

Au programme

01 Une réglementation européenne foisonnante (DORA, NIS2) (5 min)

02 Le RGPD pour les associations (35 min)

03 Questions - réponses (10 min)

Bouclier Cyber UE

Une réglementation européenne foisonnante

Bouclier Cyber UE

Des règlements et directives multiples

- RGPD : Règlement Européen sur la Protection des Données
- CSA : Cyber Security Act
- DORA : Digital Operational Resilience Act
- NIS 2 : Network and Information Security
- DMA : Digital Markets Act
- DAS : Digital Services Act
- DGA : Data Governance Act
- DA : Data Act
- AIA : Artificial Intelligence Act
- CSA : Cyber Solidarity Act
- CRA : Cyber Resilience Act

Focus sur
NIS 2 - DORA - RGPD

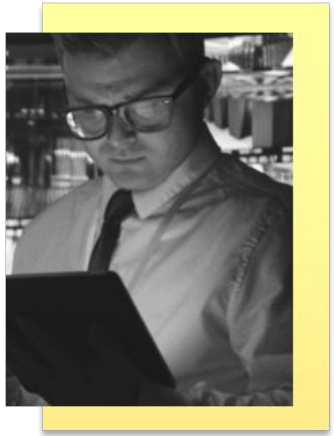
	RGPD	DORA	NIS 2
Entrée en application	Mai 2018	Janvier 2025	Octobre 2024
Entités concernées	Entités publiques et privées traitant des données personnelles	Large éventail d'entités financières Prestataires opérant des services financiers	Entités essentielles Entités importantes
Autorités de régulation	CNIL	AMF Banque de France	ANSSI

Fragmentation de l'action publique : multiplication des guichets / autorités

Le RGPD

pour les associations

Pourquoi se conformer ?



Eviter les sanctions financières, administratives et/ou réputationnelles

Respect de la vie privée

Préserver la sécurité et la confidentialité des données

Renforcer l'image et la confiance :

- Des partenaires
- Des adhérents

Un peu d'histoire

1978

Loi Informatique et Libertés

Loi française qui réglemente la liberté de traitement des données personnelles

1995

Directive européenne 95/46/CE

Texte de référence de l'Union Européenne relatif à la protection des données

2002

ePrivacy

Directive concernant le respect de la vie privée et la protection des données dans les communications électroniques

2004

Loi du 6 août 2004

Loi modifiant la loi I&L

2016

RGPD / Loi du 20 juin 2018 modifiant la loi I&L

Entrée en vigueur du règlement européen relatif à la protection des données personnelles

2018

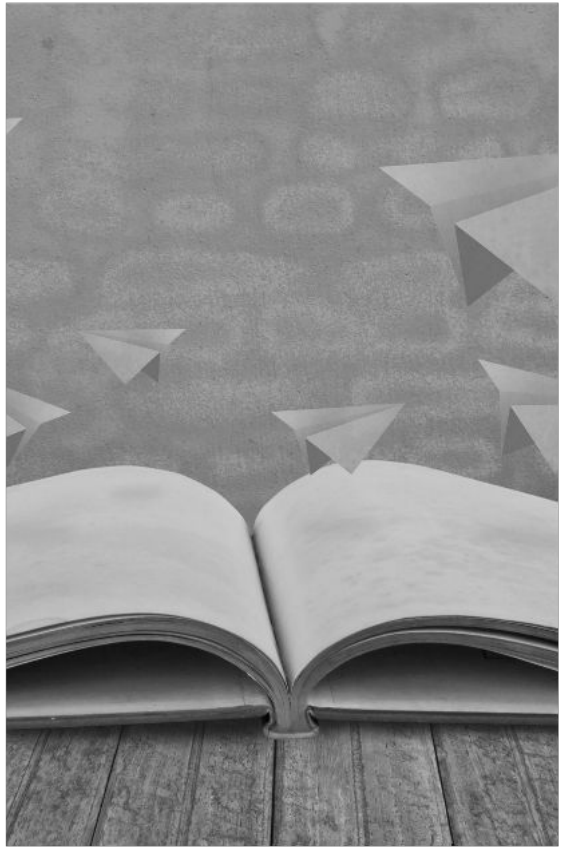
Le RGPD devient applicable

Données personnelles

Information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement.

Les données personnelles peuvent être catégorisées de la manière suivante :

- Données d'identification (nom, prénom, adresse, mail, date de naissance, photo, etc.)
- Données de vie personnelle (nombre d'enfant, situation familiale, etc.)
- Données de vie professionnelles (fonction, service, etc.)
- Données de connexion (adresse IP, logs, etc.)
- Données financières et économique (revenus, taux d'imposition, etc.)
- Données de localisation (coordonnées géographiques, etc.)



Données sensibles

C'est une information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle.

Sont considérées comme des données sensibles :

- Les opinions politiques, philosophique ou religieuses
- Les données concernant la santé
- Les données concernant la vie sexuelle ou l'orientation sexuelle
- Le numéro de sécurité social (NIR)
- Les origines raciales ou ethniques
- Les appartenances syndicales
- Les données biométriques
- Les données génétiques
- Les informations en rapport avec la police
- Les informations relatives aux infractions, condamnations ou mesures de sûreté

Où se trouvent les données ?

Les données sont partout !

Dans nos armoires, bureaux, cartons

Dans nos imprimantes

Sur les réseaux (Wifi, interne, etc.)

Sur nos clés USB

Sur nos postes de travail

Dans nos poubelles

Qu’est-ce qu’un traitement de données ?

Un traitement de données est une opération ou ensemble d’opérations effectuées ou non à l’aide de procédés automatisés appliquées à des données ou des ensembles de données.

Il peut s’agit de :

- La collecte
- La communication
- L’enregistrement
- L’organisation
- La conservation
- La modification
- L’effacement
- La consultation
- Leur utilisation

Ce qui change

Vous l'avez compris, la protection des données à caractère personnel ce n'est pas nouveau, mais avec le RGPD il y a des changements !

Le principe d'*Accountability* ou de Responsabilité

Avant le RGPD

- Déclaration des traitements de données à caractère personnel auprès de la CNIL (long, lourdeur administrative, etc.)

Depuis le RGPD

- Introduction d'un régime de responsabilité, qui impacte également les sous-traitants !
- Les traitements ne sont plus à déclarer à CNIL, mais à tenir dans un registre interne à l'entreprise
- Le but est de rendre les entreprises activement responsables de la mise en conformité des traitements et d'être capable de démontrer cette conformité

Ce qui change : De nouveaux droits

Chaque personne concernée par un traitement doit en être informée de manière concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Elle peut également exercer les droits suivants.

Anciens droits, toujours d'actualité

- Le droit d'accès
- Le droit à la rectification
- Le droit à l'effacement (ou à l'oubli)
- Le droit à l'opposition

Et le RGPD a introduit :

- Le droit à la limitation d'un traitement
- Le droit à ne pas être sujet au profilage ou aux décisions automatisées
- Le droit à la portabilité

Si une personne vous fait parvenir son souhait d'exercer un de ses droits, vous avez 30 jours pour y répondre !

Parmi les réponses suivantes, lesquelles sont des données personnelles ?

A

Le numéro de téléphone professionnel

B

La date de naissance

C

Photo d'identité

D

Le nombre de congés d'un collaborateur

Parmi les réponses suivantes, lesquelles sont des données personnelles ?

A

Le numéro de téléphone professionnel

B

La date de naissance

C

Photo d'identité

D

Le nombre de congés d'un collaborateur

Parmi les réponses suivantes, laquelle n'est pas un « traitement de données personnelles » au sens du RGPD?

A

La gestion du registre du personnel

B

L'enregistrement des données clients

C

La gestion du stock de fourniture

D

L'utilisation de la liste des prospects

Parmi les réponses suivantes, laquelle n'est pas un « traitement de données personnelles » au sens du RGPD?

A

La gestion du registre du personnel

B

L'enregistrement des données clients

C

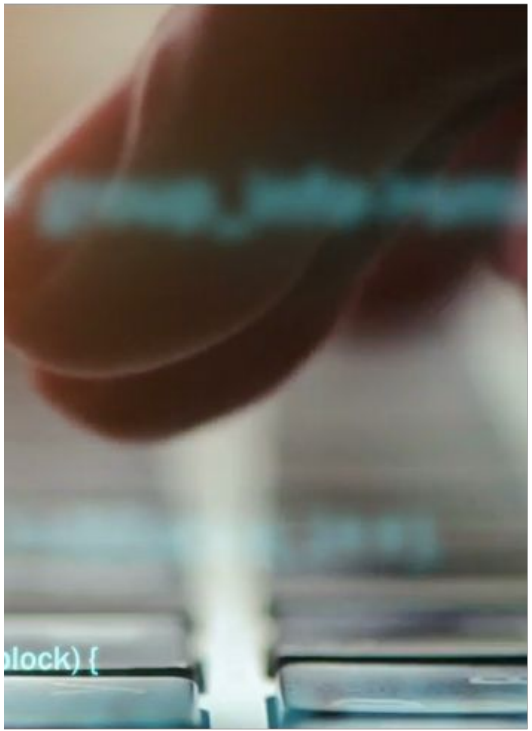
La gestion du stock de fourniture

D

L'utilisation de la liste des prospects

La conformité des traitements des données personnelles

Le responsable de traitement



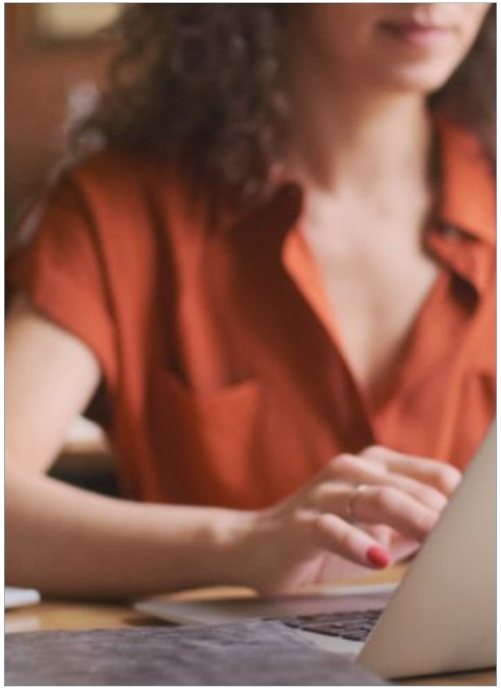
Le responsable de traitement est la personne morale ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser, Il s'agit très souvent du Président de l'association

Le responsable de traitement doit s'assurer que son traitement est inscrit au registre des traitements de l'association

Le registre des traitements

- répertorie tous les traitements, ceux en tant que Responsable de traitement mais aussi ceux en tant que sous-traitant
- doit contenir : les finalités, les durées de conservation, la base légale, les mesures de protections, les acteurs, les transferts, etc.

Le traitement



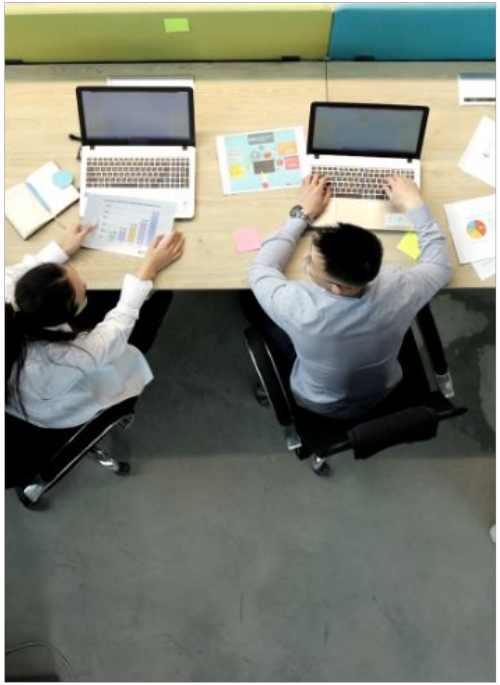
Loyal et transparent

- Les personnes concernées par le traitement doivent être informées du sort de leurs données par un langage clair et simple
- Elles doivent être informées des risques, des règles, des garanties et des droits

Licite

- Pour qu'un traitement existe, il doit être basé sur une des 6 bases légales :
  - Le consentement de la personne concernée
  - Nécessaire dans le cadre d'un contrat ou de l'intention d'en conclure un
  - Respect d'une obligation légale
  - Sauvegarde des intérêts vitaux
  - Exécution d'une mission de service public ou relevant de l'autorité publique
  - Intérêt légitime

La collecte



Finalité déterminée, explicite et légitime

- Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

Données adéquates, pertinentes et limitées

- Il s'agit du principe de minimisation des données : je collecte seulement ce dont j'ai besoin pour la finalité de mon traitement !

Données exactes et tenues à jour

- Les données à caractère personnel doivent être collectées de manière exactes et, si nécessaire, tenues à jours. Les données qui sont inexactes doivent être soient rectifiées ou effacées sans tarder.

Vigilance sur les zones de libres commentaires !

- Les personnes concernées doivent être informées de la collecte de leurs données personnelles
- Les informations renseignées ne doivent pas porter atteinte à l'image de la personne ou l'empêcher de bénéficier d'une prestation à laquelle elle peut prétendre
- La personne concernée peut à tout moment exercer son droit d'accès et lire ces commentaires

Les durées de conservation

Collecter oui, mais pas pour toujours !

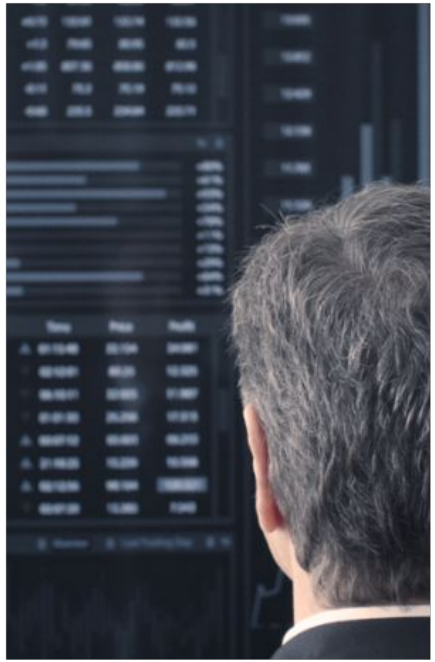
La durée doit être déterminée avant même la collecte et peut être définie ou recommandée par l'autorité de contrôle

Elle doit être communiquée au sous-traitant s'il y a lieu

Le temps nécessaire au traitement et pendant une durée déterminée

Par exemple :

- Le dossier administratif du personnel est conservé jusqu'au départ du collaborateur dans l'entreprise
- Le dossier disciplinaire du collaborateur est conservé 1 an à compter de la cessation de ses fonctions



Où les traitements de données à caractère personnel doivent-ils être inscrits ?

A
Dans le registre des traitements

B
Dans le dossier des collaborateurs

C
A la CNIL

D
Ils ne doivent pas être inscrits

Où les traitements de données à caractère personnel doivent-ils être inscrits ?

A
Dans le registre des traitements

B
Dans le dossier des collaborateurs

C
A la CNIL

D
Ils ne doivent pas être inscrits

Le traitement qui a pour finalité « la gestion des adhésions » est basé sur quelle base légale ?

A

Consentement

B

Exécution d'un contrat

C

Obligation légale

D

Intérêt légitime

Le traitement qui a pour finalité « la gestion des adhésions » est basé sur quelle base légale ?

A

Consentement

B

Exécution d'un contrat

C

Obligation légale

D

Intérêt légitime

Parmi ces informations, lesquelles doivent figurer dans le registre de traitement ?

A

La liste nominative des personnes concernées par le traitement

B

L'identification du responsable de traitement

C

La finalité du traitement

D

Les mesures de sécurité mises en place

Parmi ces informations, lesquelles doivent figurer dans le registre de traitement ?

A

La liste nominative des personnes concernées par le traitement

B

L'identification du responsable de traitement

C

La finalité du traitement

D

Les mesures de sécurité mises en place

Quelques aspects sécurité mis en avant par le RGPD

Le privacy by design

Définir la durée de conservation

Prendre en compte la mise en œuvre du consentement (si éligible)

Etudier la nécessité d'une analyse d'impact

Prendre en compte la disponibilité, la confidentialité et l'intégrité des données tout au long du traitement

Assurer une information transparente pour la personne concernée

Prendre en compte le droit des personnes (accès, modification, suppression,…)

Etude d'impact sur la vie privée

Lorsqu'un traitement est susceptible d'atteinte aux droits et libertés des personnes concernées il doit faire l'objet d'une analyse d'impact sur la vie privée (EIVP ou AIPD ou PIA).

Une EIVP est obligatoire pour tout traitement ayant au moins 2 des critères suivants :

- Évaluation/scoring (y compris le profilage) ;
- Décision automatique avec effet légal ou similaire ;
- Surveillance systématique ;
- Collecte de données sensibles ;
- Collecte de données personnelles à large échelle ;
- Croisement de données ;
- Personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- Usage innovant (utilisation d'une nouvelle technologie) ;
- Exclusion du bénéfice d'un droit/contrat.

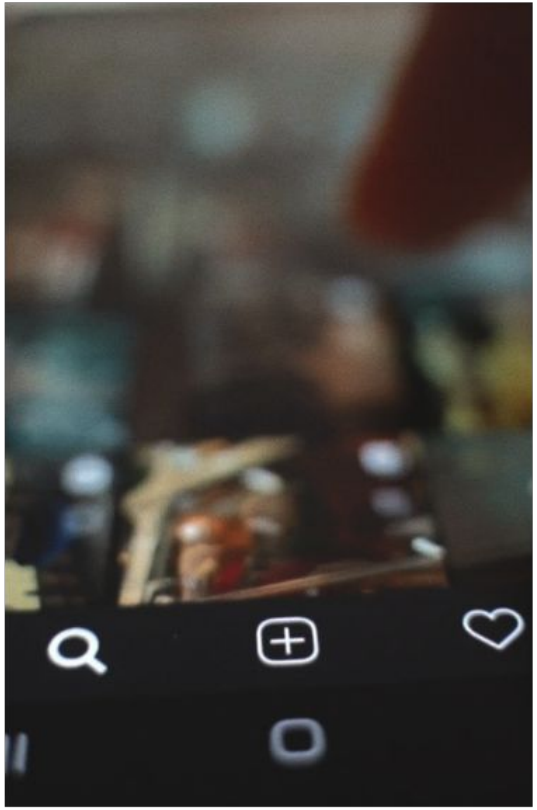
La violation de donnée

La violation de données à caractère personnel se définit comme la violation de sécurité entrainant la destruction, la perte, l'altération, la divulgation des données à caractère personnel traitées

Je suis victime ou témoin d'une violation : j'informe au plus vite le responsable de traitement

Le délai est de 72h pour notifier la violation à la CNIL et les personnes concernées s'il y a un risque élevé pour leurs droits et libertés

Des mesures doivent être prises pour remédier à la violation le cas échéant, pour limiter les conséquences négatives de la violation



Je souhaite mettre en place un nouveau traitement, quand dois-je définir les durées de conservation des données que je vais traiter ?

A

Dès la conception de mon projet

B

Dès que je collecte les premières données

C

Dès que mon projet est opérationnel

D

Quand j'aurai le temps

Je souhaite mettre en place un nouveau traitement, quand dois-je définir les durées de conservation des données que je vais traiter ?

A

Dès la conception de mon projet

B

Dès que je collecte les premières données

C

Dès que mon projet est opérationnel

D

Quand j'aurai le temps

Par erreur, je transfère un fichier par mail contenant les données personnelles de plusieurs adhérents à un membre de l'association, que dois-je faire ?

A

Je ne fais rien

B

Je signale au destinataire que c'est une erreur et c'est tout

C

Je préviens le client concerné

D

Je préviens le président le plus rapidement possible

Par erreur, je transfère un fichier par mail contenant les données personnelles de plusieurs adhérents à un membre de l'association, que dois-je faire ?

A

Je ne fais rien

B

Je signale au destinataire que c'est une erreur et c'est tout

C

Je préviens le client concerné

D

Je préviens le président le plus rapidement possible

Je reçois par email un lien d'une personne que je ne connais pas. Je…

A Clique sur le lien

B J'informe la CNIL

C J'ignore le mail

D Je supprime le mail

Je reçois par email un lien d'une personne que je ne connais pas. Je…

A Clique sur le lien

B J'informe la CNIL

C J'ignore le mail

D Je supprime le mail

Qu’est-ce qu’une violation de données ?

A La perte des données

B La divulgation des données

C L’altération des données

D La destruction des données

Qu’est-ce qu’une violation de données ?

A La perte des données

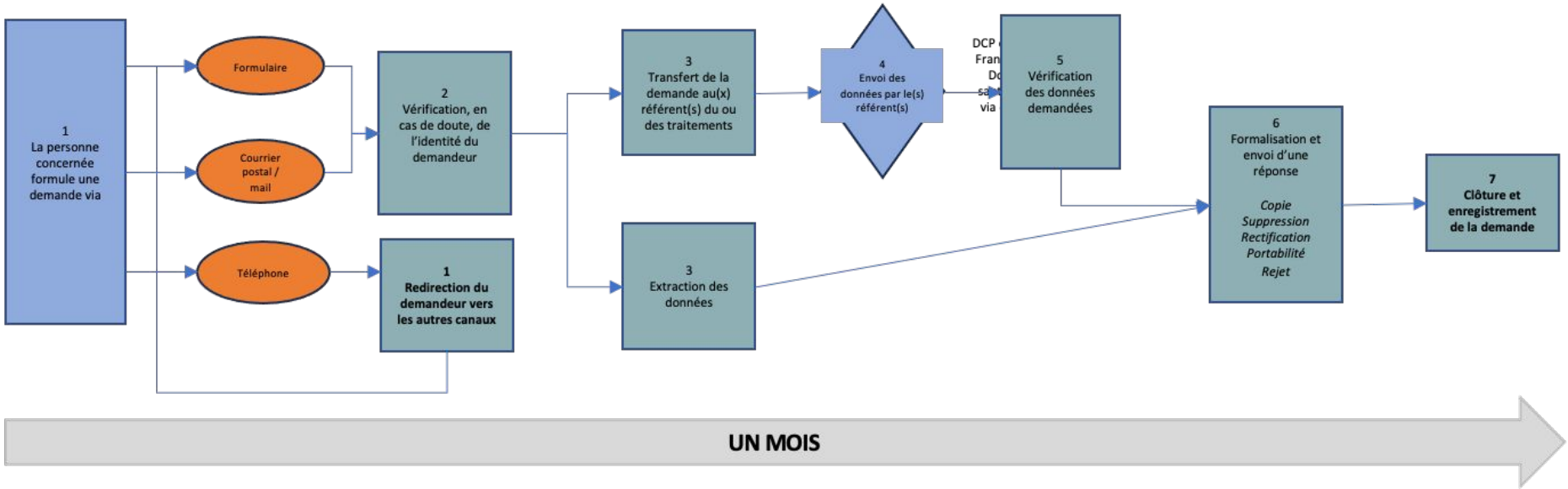
B La divulgation des données

C L’altération des données

D La destruction des données

Répondre à une demande d'exercice des droits

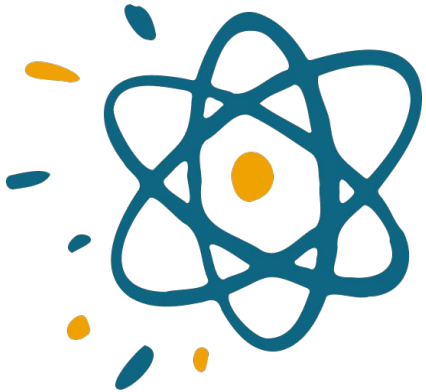
Priorité 2024 de la CNIL


1
La personne concernée formule une demande via
Formulaire
Courrier postal / mail
Téléphone
2
Vérification, en cas de doute, de l'identité du demandeur
1
Redirection du demandeur vers les autres canaux
3
Transfert de la demande au(x) référent(s) du ou des traitements
3
Extraction des données
4
Envoi des données par le(s) référent(s)
5
Vérification des données demandées
6
Formalisation et envoi d'une réponse
Copie
Suppression
Rectification
Portabilité
Rejet
7
Clôture et enregistrement de la demande
UN MOIS

Des questions ?

On vous répond !

La suite du programme



Et si on se rencontrait ?

1h de conseil, gratuite et renouvelable

Un·e spécialiste numérique vous aide
à appliquer concrètement
ce que vous avez appris aujourd'hui !

Je m'inscris (2 min) :
https://bit.ly/demande-conseil-cyber

Pas de prérequis ni de préparation

Exemples de sujets qui peuvent être traités pendant l'heure :

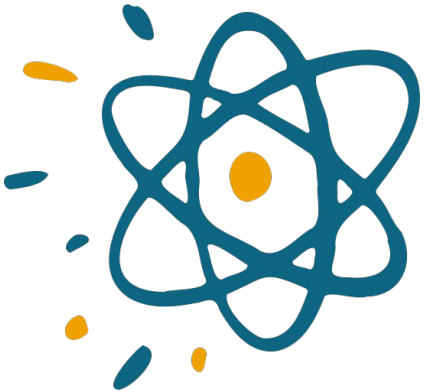
- ➔ Audit de cybersécurité de son association
- ➔ Sécurisation de son site web
- ➔ ...

Merci !

cyberforgood.fr

DORA

Digital Operational Resilience Act



DORA Qu'est ce que c'est ?

Le Digital Operational Resilience Act (DORA) est une législation proposée pour renforcer la résilience opérationnelle dans le domaine numérique.

Ce qu’il faut savoir

Les objectifs les entités visées ainsi que les exigences clés

Objectifs et enjeux de DORA

Renforcer la Sécurité

DORA vise à renforcer la sécurité des opérations financières numériques contre les menaces

Assurer la Résilience

Elle cherche à garantir la résilience des systèmes dans des situations de stress opérationnel.

Protéger les Intérêts

Cela protège les intérêts des consommateurs et des parties prenantes du secteur financier.

NIS 2

Network and Information Security

NIS 2 – Changement de paradigme

Adoption de NIS 1 en 2016, transposée en 2018

=> Objectif initial : augmenter le niveau de cybersécurité des acteurs majeurs de 10 secteurs stratégiques

- Opérateurs d'Importance Vitale (OIV) : indispensables pour la nation (eau, énergie, …)
- Opérateurs de Service Essentiel (OSE) : service essentiel, tributaire de SI dont les FSN

=> Obligations principales : réduire l'exposition de leurs SI, notifier les incidents

Adoption de NIS 2 en 2022, une opportunité unique pour :

=> Elargir la protection cyber (d'une centaine à plusieurs milliers d'entités)

=> Renforcer la coopération entre Etats par un cadre formel (réseau CyCLONe)

=> mobiliser largement le tissu économique national et le secteur public

Extension sans précédent en matière de règlementation cyber

NIS 2

Pour qui ?

NIS 2 – Extension du périmètre

Schématisation simplifiée de classification selon règles de principe

Taille de l'entité	Nb d'employés		CA (millions d'€)		Bilan annuel (millions d'€)		Annexe 1 sectorielle	Annexe 2 sectorielle
Intermédiaire & grande	> 250		≥ 50		≥ 43		**Entités essentielles**	**Entités importantes**
Moyenne	≥ 50	≤ 250	≥ 10	> 50	≥ 10	> 43	**Entités importantes**	**Entités importantes**
Micro & petite	< 50		> 10		< 10		***Non concernées***	***Non concernées***

Principales catégories sectorielles

Infrastructures numériques sans condition de taille	**Annexe 1 et 2**	**Infrastructures numériques**
Fournisseurs de réseaux de communications électroniques publics, de services de communications électroniques accessibles au public et prestataires de services de confiance	Energies, Transports, Santé, Etablissements de crédits, Marchés financiers, Administrations publiques	Fournisseurs de points d'échange internet, de services DNS, de services cloud, de services de centres de données, de réseaux de diffusion de contenu

NIS 2

Pour quoi ?

NIS 2 – Nouvelles obligations

Exigences adaptées et proportionnées aux enjeux de chacune des catégories d'entités (EE et EI)

Engagement des entités à se conformer à des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées, fondées sur une approche tous risques

- Politiques relatives à l'analyse des risques et à la sécurité des SI
- Gestion des incidents
- Continuité des activités (gestion des sauvegardes, reprise des activités, gestion des crises)
- Sécurité de la chaîne d'approvisionnement (incluant les relations entre entités et tiers)
- Sécurité de l'acquisition, du développement et de la maintenance des réseaux et SI politiques et procédures pour évaluer l'efficacité des mesures
- Pratiques de base en matière de cyber hygiène et formation à la cybersécurité
- Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
- Sécurité des RH, des politiques de contrôle d'accès et la gestion des actifs
- Utilisation de solutions d'authentification à plusieurs facteurs (communications vocales et vidéo)

NIS 2
Pour quand ?

NIS 2 – Transposition nationale

Entrée en vigueur 21 mois après sa publication, soit au plus tard le 27 octobre 2024

Application partielle : certaines exigences seront d'application directe, d'autres seront soumises à un délai de mise en conformité

Deux phases :

- **Phase de préparation du projet de loi en vue de sa présentation au Parlement et de son adoption au plus tôt pendant l'année 2024 (1er semestre)**
- **Phase de production des décrets et arrêtés, soumis à validation interministérielle en vue d'une publication un mois après le projet de loi**

Renforcement du régime de sanctions (entre 1,4 et 2% du CA) précédé et doublé d'un accompagnement de l'ANSSI par des actions de sensibilisation et, si nécessaire, la mise à disposition de nouveaux outils (portail numérique proposant des solutions de sécurisation)

En synthèse

	RGPD	DORA	NIS 2
Entrée en application	Mai 2018	Janvier 2025	Octobre 2024
Entités concernées	Entités publiques et privées traitant des données personnelles	Large éventail d'entités financières Prestataires opérant des services financiers	Entités essentielles Entités importantes
Autorités de régulation	CNIL	AMF Banque de France	ANSSI

Fragmentation de l'action publique : multiplication des guichets / autorités