

**Denis JACOPINI sur Europe 1 parle de son livre « CYBERARNAQUES S'informer pour mieux se protéger » ce jeudi 12 avril 2018 en direct dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel WIZMAN**



DENIS JACOPINI - MARIE NOCENTI

# CYBER ARNAQUES

## S'INFORMER POUR MIEUX SE PROTÉGER

PLON

Denis JACOPINI sur Europe 1 parle de son livre « CYBERARNAQUES ». Informer pour mieux se protéger » ce jeudi 12 avril 2018 en direct dans « Bonjour la France » avec Daphné BURKI et Ariel WIZMAN

Internet et les réseaux sociaux ont envahi notre quotidien, pour le meilleur mais aussi pour le pire.. Qui n'a jamais reçu de propositions commerciales pour de célèbres marques de luxe à prix cassés, un email d'appel au secours d'un ami en vacances à l'autre bout du monde ayant besoin d'argent ou un mot des impôts informant qu'une somme substantielle reste à rembourser contre la communication de coordonnées bancaires ? La Toile est devenue en quelques années le champ d'action privilégié d'escrocs en tout genre à l'affût de notre manque de vigilance. Leur force ? Notre ignorance des dangers du Net et notre « naïveté » face aux offres trop alléchantes qui nous assaillent. Denis JACOPIN en parle ce jeudi 14 avril 2018 en direct sur Europe 1 dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel Wizman

<http://www.europe1.fr/emissions/bonjour-la-france>

DENIS JACOPINI - MARIE NOCENTI

# CYBER ARNAQUES

## S'INFORMER POUR MIEUX SE PROTÉGER

PLON

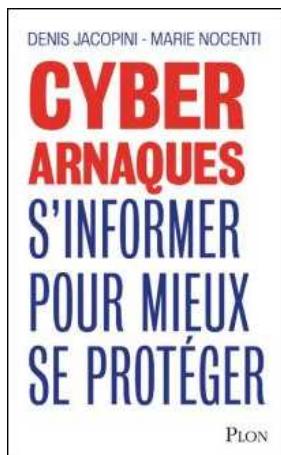
Plutôt qu'un inventaire, Denis Jacopini, avec la collaboration de Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en évitez les conséquences parfois dramatiques.. et coûteuses.

Un livre indispensable pour « surfer » en toute tranquillité ! Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier. Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques. Marie Nocenti est romancière.

[block id="24761" title="Pied de page HAUT"]

---

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)  
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur [Fnac.fr](http://Fnac.fr)

---

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

---

Commandez sur Fnac.fr

---

[https://youtu.be/usg12zkRD9I?list=UUoHqj\\_HKcbzRuvIPdu3FktA](https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA)

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr

---



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur [Fnac.fr](https://www.fnac.fr)

Source : *Cyberarnaques S'informer pour mieux se protéger – broché – Denis Jacopini, MARIE NOCENTI – Achat Livre – Achat & prix | fnac*

---

# Un employeur peut-il consulter les courriels d'une messagerie professionnelle d'un de ses salariés ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



**Un employeur peut-il consulter les courriels d'une messagerie professionnelle d'un de ses salariés ?**

**Un employeur peut-il consulter les courriels d'une messagerie professionnelle d'un de ses salariés ?**

« L'employeur ne peut, hors présence du salarié, consulter ses messages sans son autorisation. Car, potentiellement, il pourrait y trouver des messages dits «personnels». Le principe, c'est qu'une messagerie ne peut pas être 100 % professionnelle. Quand on écrit un message à son conjoint pour le prévenir qu'on va être en retard par exemple. C'est donc toléré mais il ne faut pas en abuser. La seule condition pour l'employeur est dans le cas d'un danger grave : concurrence déloyale ou terrorisme. Mais, dans ce cas, cela nécessite la présence d'un huissier. »

[block id="24761" title="Pied de page HAUT"]

**Quelques articles sélectionnés par nos Experts :**

Quels sont les droits et devoirs des salariés en matière de

sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

---

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD** ? ?

Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?

Contactez-nous

---



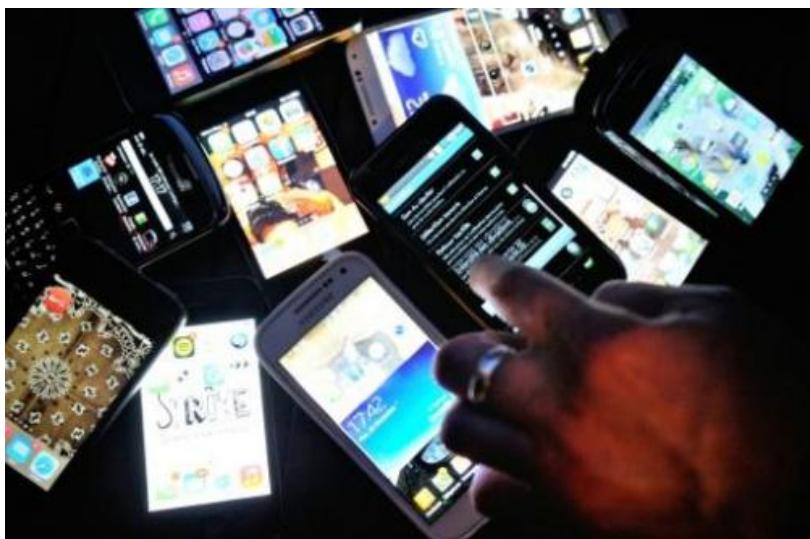
Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

*« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».*

Source : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord

---

# Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?



Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

---

## Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

Dès lors que le téléphone du salarié est professionnel, l'employeur a ce droit, à moins d'avoir mentionné avant le message «personnel». Dans ce cas, l'employeur n'a plus le droit. Mais souvent, on n'oublie de l'écrire... »

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord

# Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ?

 <p>Denis JACOPINI VOUS INFORME LCI</p>	<p>Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? #1</p>
--	--

## Un employeur peut-il consulter les courriels d'une messagerie professionnelle d'un de ses salariés ?

« L'employeur ne peut, hors présence du salarié, consulter ses messages sans son autorisation. Car, potentiellement, il pourrait y trouver des messages dits «personnels». Le principe, c'est qu'une messagerie ne peut pas être 100 % professionnelle. Quand on écrit un message à son conjoint pour le prévenir qu'on va être en retard par exemple. C'est donc toléré mais il ne faut pas en abuser. La seule condition pour l'employeur est dans le cas d'un danger grave : concurrence déloyale ou terrorisme. Mais, dans ce cas, cela nécessite la présence d'un huissier. »

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord

# Cyberarnaques S'informer pour mieux se protéger – Denis Jacopini, Marie Nocenti | fnac

DENIS JACOPINI - MARIE NOCENTI

# CYBER ARNAQUES S'INFORMER POUR MIEUX SE PROTÉGER

PLON

Cyberarnaques  
S'informer  
pour mieux se  
protéger

Internet et les réseaux sociaux ont envahi notre quotidien, pour le meilleur mais aussi pour le pire... Qui n'a jamais reçu de propositions commerciales pour de célèbres marques de luxe à prix cassés, un email d'appel au secours d'un ami en vacances à l'autre bout du monde ayant besoin d'argent ou un mot des impôts informant qu'une somme substantielle reste à rembourser contre la communication de coordonnées bancaires ? La Toile est devenue en quelques années le champ d'action privilégié d'escrocs en tout genre à l'affût de notre manque de vigilance. Leur force ? Notre ignorance des dangers du Net et notre « naïveté » face aux offres trop alléchantes qui nous assaillent.

DENIS JACOPINI - MARIE NOCENTI

# CYBER ARNAQUES S'INFORMER POUR MIEUX SE PROTÉGER

PLON

Plutôt qu'un inventaire, Denis Jacopini, avec la collaboration de Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en éviter les conséquences parfois dramatiques... et coûteuses.

Un livre indispensable pour « surfer » en toute tranquillité ! Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier.

Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillages de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques.

Marie Nocenti est romancière.

Commandez CYBERARNAQUES sur le site de la FNAC (disponible à partir du 29/03/2018)

## LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX - MISE EN CONFORMITÉ)
  - ANALYSE DE VOTRE ACTIVITÉ
  - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
  - IDENTIFICATION DES RISQUES
  - ANALYSE DE RISQUE (PIA / DPIA)
  - MISE EN CONFORMITÉ RGPD de vos traitements
  - SUIVI de l'évolution de vos traitements
  - FORMATIONS / SENSIBILISATION :
    - CYBERCRIMINALITÉ
  - PROTECTION DES DONNÉES PERSONNELLES
    - AU RGPD
    - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (réécriture de Photos / SMS)
  - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
  - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
    - SÉCURITÉ INFORMATIQUE
    - SYSTÈMES DE VOTES ÉLECTRONIQUES

### Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en Cybercriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »

« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formation (et sensibilisation) à la Cybercriminalité (Autorisation n°93 04 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques d'judiciaires ;
- Recherche de preuve (téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;

Le Net Expert  
INFORMATIQUE

Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Cyberarnaques S'informer pour mieux se protéger – broché – Denis Jacopini, MARIE NOCENTI – Achat Livre – Achat & prix | fnac*

# GDPR compliance: Request for costing estimate

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



**LE NET EXPERT**  
AUDITS & EXPERTISES

**EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES**  
**LE NET EXPERT**  
*.fr*

**RGPD CYBER**  
**LE NET EXPERT**  
MISES EN CONFORMITÉ

**SPY DETECTION**  
Services de détection de logiciels espions

**LE NET EXPERT FORMATIONS**

**LE NET EXPERT**  
ARNAQUES & PIRATAGES

**GDPR compliance: Request for costing estimate**



LeNetExpert

You seem to express an interest in the GDPR (perhaps a little by obligation) and you want to tell us about a project. We thank you for your confidence.

Intervening on Data Protection missions since 2012, after having identified different types of expectations, we have adapted our offers so that they best meet your needs.

Thus, we can assist you in bringing your structure into compliance in several ways :

1. Are you looking for autonomy ?

We can assist you to learn the essentials of European regulations relating to the Protection of Personal Data and the necessary to understand and start a compliance. Once the training is completed, you are independent but can always count on our support either in the form of personalized training, or in the form of personalized support;

At the end of this training, we will give you a certificate proving the implementation of a process to bring your establishment into compliance with the GDPR (General Data Protection Regulations). For information, we are referenced to the CNIL.

2. Do you want to be accompanied for the implementation of compliance ?

We carry out for you the audit which will highlight the points to be improved. At the end of this stage you can, if you wish, achieve compliance or let us proceed with the improvements that you have validated;

At the end of this audit, we will give you a report proving the implementation of corrections as part of your process to bring your establishment into compliance with the GDPR (General Data Protection Regulations).

In a perfectly complementary way with your IT service provider and possibly with your legal department, we can take care of the entire process of bringing your establishment into compliance with the GDPR (General Data Protection Regulation) and the various regulations relating to the protection of Personal Data.

From the audit to the follow-up, you can count on our technical and educational expertise so that your establishment is supported externally.

In order to send you a personalized proposal adapted both to the needs of your structure, in accordance with your strategy and your priorities, we would like you to answer these few questions :

**We guarantee extreme confidentiality on the information communicated. Persons authorized to consult this information are subject to professional secrecy.**

Do not hesitate to communicate as many details as possible, this will allow us to better understand your expectations.

Your First Name / NAME (required)

Your Organization / Company (required)

Your email address (required)

A telephone number (will not be used for commercial prospecting)

You can write us a message directly in the free text area. However, if you want us to establish precise costing for you, we will need the information below.

In order to better understand your request and establish a quote, please provide us with the information requested below and click on the "Send entered informations" button at the bottom of this page for us to receive it. You will receive an answer quickly.

#### YOUR ACTIVITY

Details about your activity :

Are you subject to professional secrecy?

Yes  No  I don't know

Does your activity depend on regulations?

Yes  No  I don't know

If "Yes", which one or which ones?

#### YOUR COMPUTER SYSTEM

Can you describe the composition of your computer system. We would like, in the form of an enumeration, to know the equipment which has any access to personal data with for each device ALL the software (s) used and their function (s) .

Examples :

- 1 WEB server with website to publicize my activity;

- 1 desktop computer with billing software to bill my clients;

- 2 laptops including:

> 1 with email software to correspond with clients and prospects + word processing for correspondence + billing software to bill my clients ...

> 1 with email software to correspond with customers and prospects + accounting software to do the accounting for my company ;

- 1 smartphone with email software to correspond with customers and prospects.

Yes  No  I don't know

Do you have one or more websites?

Yes  No  I don't know

What is (are) this (these) website (s)?

Yes  No  I don't know

Do you have data in the Cloud?

Yes  No  I don't know

Which cloud providers do you use?

#### YOUR PERSONAL DATA PROCESSING

If you have already established it, could you provide us with the list of processing of personal data (even if it is incomplete)?

#### SIZING YOUR BUSINESS

Number of employees in your structure :

1

2

3

How many of these employees use computer equipment ?

1

2

3

Number of departments or departments \*\* in your structure (example: Commercial service, technical service ...) :

Please list the services or departments \*\* of your structure:

#### SERVICE PROVIDERS & SUBCONTRACTORS

Do you work with sub-contractors?

Yes  No  I don't know

Please list these subcontractors :

1

2

3

Do you work with service providers who work on your premise or in your agencies (even remotely) ?

Yes  No  I don't know

Please list these providers :

1

2

3

How many IT companies do you work with ?

Please list these IT companies indicating the products or services for which they operate and possibly their country of establishment :

#### YOUR SITUATION TOWARDS THE GDPR

Does your establishment exchange data with foreign countries ?

Yes  No  I don't know

If "Yes", with which countries?

Yes  No  I don't know

Have you already been made aware of the GDPR ?

Yes  No  I don't know

Have people using IT equipment already been made aware of the GDPR ?

Yes  No  I don't know

If you or your employees have not been made aware of the GDPR, would you like to undergo training ?

Yes  No  I don't know

#### YOUR WORKPLACE

The analysis of the data processing conditions in your professional premises or your professional premises is part of the compliance process.

Do you have several offices, agencies etc. legally dependent on your establishment ?

Yes  No

If "Yes", how much ?

1

2

3

In which city (ies) (and country if not in France) do you or your employees work ?

#### TYPE OF SUPPORT DESIRED

We can support you in different ways.

A) We can teach you to become autonomous (training) ;

B) We can support you at the start and then help you become independent (support, audit + training) ;

C) We can choose to entrust us with the entire process of compliance (support) ;

D) We can accompany you in a personalized way (thank you to detail your expectations).

What type of support do you want from us (A / B / C / D + details) ?

#### END OF QUESTIONNAIRE

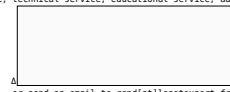
If you wish, you can send us additional information such as:

- Emergency of your project;

- Any additional information that you deem useful to allow us to better understand your project.

[block id="24086" title="Mentions légales formulaires"]

\*\* = for example, commercial service, technical service, educational service, administrative and financial service ...



Denis JACOPINI is our Expert who will accompany you in your compliance with the GDPR.

Let me introduce myself: Denis JACOPINI. I am an expert in sworn IT and specialized in GDPR (protection of Personal Data) and in cybercrime. Consultant since 1996 and trainer since 1998, I have experience since 2012 in compliance with the regulations relating to the Protection of Personal Data. First technical training, CNIL Correspondent (CIL: Data Protection Correspondent) then recently Data Protection Officer (DPO n° 15845), as a compliance practitioner and trainer, I support you in all your procedures for compliance with the GDPR.

« My goal is to provide all my experience to bring your establishment into compliance with the GDPR. »

---

# RGPD : Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité ?



RGPD : Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité ?

---

Le Net Expert : Denis JACOPINI, vous êtes spécialisé dans l'accompagnement des PME dans la mise en conformité avec le RGPD depuis plusieurs années. Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité avec le RGPD ?

Si le 25 mai 2018 vous n'avez pas terminé votre mise en conformité avec le RGPD ou pire, vous venez à peine de l'initier pour votre entreprise, association ou administration, stricto sensu, en tant que responsable de traitement pénallement responsable, vous devenez amenable et les sanctions encourues, forcément pécuniaires selon les cas, pourraient être accompagnées de peines de prison comme le précise l'article 226-17 du Code pénal.

Ainsi, le Règlement sera « obligatoire dans tous ses éléments et directement applicable dans tout état membre », dont la France dès le 25 mai 2018, et puisqu'il s'agit d'un règlement, celui-ci entrera directement en vigueur, sans nécessiter de législation de transposition.

En réalité, avant que soient engagées des sanctions à votre encontre, vous serez contacté par la CNIL, laquelle vous demandera certainement de justifier les mesures prises à l'égard du Règlement Européen. Il est clair qu'au plus vous faites preuve de négligence, de mauvaise foi et de résistance, les sanctions risquées se rapprocheront du maximum à savoir la plus grande valeur entre 4% de votre chiffre d'affaire mondial ou 20 millions d'euros.

Si par contre, vous avez entamé une démarche de mise en conformité à savoir au minimum commencé à suivre une formation, désigné officiellement une personne (interne ou externe à votre entreprise) à cette démarche réglementaire et même si vous en êtes seulement au stade où vous avez commencé à établir la liste de vos traitements avec les risques inhérents à la vie privée et aux libertés fondamentales des propriétaires des données à caractère personnel et si possible vous avez commencé à mettre en place des mesures correctives, vous montrerez ainsi à l'autorité administrative indépendante de contrôle du bon respect de la réglementation relative à la protection des données à caractère personnel (la CNIL en France) que vous avez pris en compte cette démarche dans votre organisation, pris au sérieux des défaillances en matière juridique ou technique de votre organisation et que des améliorations sont en cours. L'ensemble des démarches accomplies même après le 25 mai 2018 joueront en votre faveur en anéantissant les risques de sanction, bien évidemment à condition que vous ne fassiez aucune victime en cas de fuite de données avant.



RGPD = RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Besoin d'un accompagnement pour vous mettre en conformité avec le RGPD ? ?

Besoin d'une formation pour apprendre à vous

mettre en conformité avec le RGPD ?

Contactez-nous

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles



Denis JACOPINI est Expert Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005);
- Expertises techniques et judiciaires (avis technico-économiques de preuves téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de CIL (Correspondants Informatique et Libertés) ;
- Formation de DPO (Délégués à la Protection des Données) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Source : Denis JACOPINI (Expert Informatique spécialisé RGPD)

# Règlement européen sur la protection des données : Transparence et

# responsabilisation



Règlement européen sur la  
protection des données  
Transparence et  
responsabilisation

**Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.**

**Une clé de lecture : la protection des données dès la conception et par défaut (privacy by design)**

Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

**Un allégement des formalités administratives et une responsabilisation des acteurs**

Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (accountability).

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

**De nouveaux outils de conformité :**

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduites
- le DPO (délégué à la protection des données)
- les études d'impact sur la vie privée (EIVP)

**Les « études d'impact sur la vie privée » (EIVP ou PIA)**

Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

Si l'organisme ne parvient pas à réduire ce risque élevé par des mesures appropriées, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

**Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements**

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures.

L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

**Le Délégué à la Protection des données (Data Protection Officer)**

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations.

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le délégué devient le véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

source : CNIL



Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs aux **risques en informatique**, découvrir et comprendre les **arnaches et les piratages informatiques** pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, pirates, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

**Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL**

# Règlement européen sur la protection des données : Renforcement des droits des personnes

Règlement européen sur la protection des données : Renforcement des droits des personnes

## Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci.

### Consentement renforcé et transparence

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambiguë.

### De nouveaux droits

Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

Des conditions particulières pour le traitement des données des enfants : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

source : CNIL



Denis Jacopini anime des conférences et des formations et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 0304184).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, conteneurs, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

# Règlement européen sur la

# protection des données : Evolution du cadre juridique



Règlement européen sur la  
protection des données  
: Evolution du cadre  
juridique

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne le 4 mai 2016 et entré en application le 25 mai 2018. L'adoption de ce texte permet à l'Europe de s'adapter aux nouvelles réalités du numérique.

## Un cadre juridique unifié pour l'ensemble de l'UE

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

### Un champ d'application étendu

#### • Le critère du ciblage

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

#### • La responsabilité des sous-traitants

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le projet de règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

### Un guichet unique : le « one stop shop »

Les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'Etat membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements transnationaux.

### Une coopération renforcée entre autorités pour les traitements transnationaux

Toutefois, dès lors qu'un traitement sera transnational – donc qu'il concerne les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernés seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G29.

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ».

Que le CEPD soit ou non saisi, l'autorité « chef de file » portera la décision ainsi partagée par ses homologues. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».

• **Par exemple**, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'Etat. Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

source : CNIL



Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL