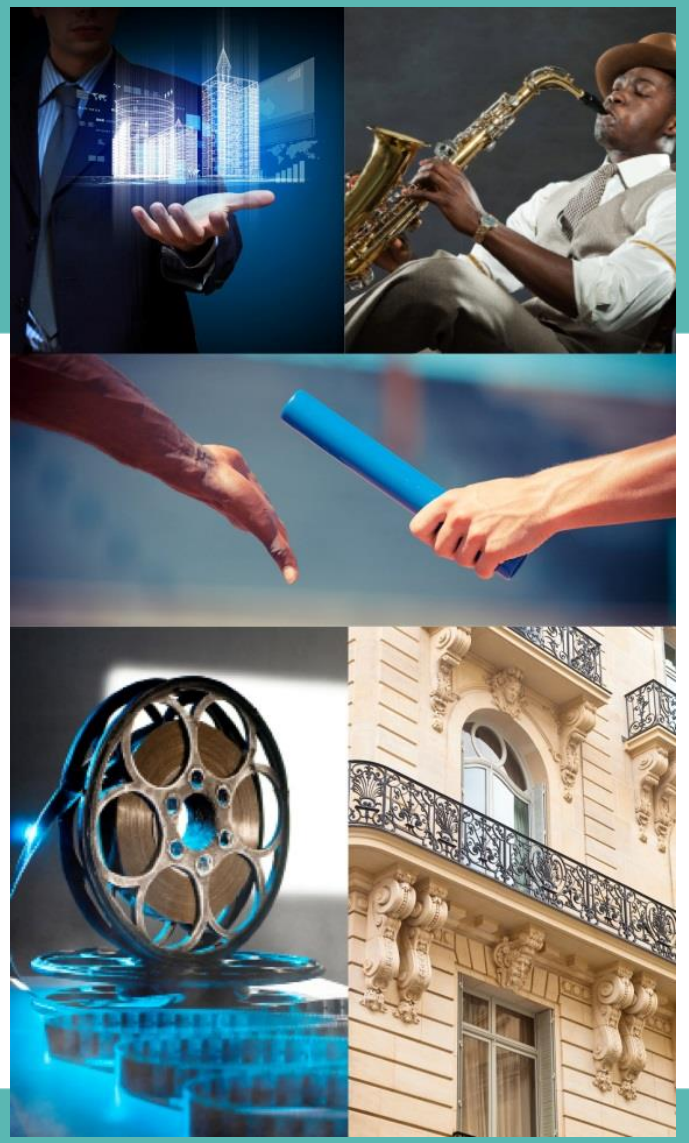
AVOCATS
BARREAU
• PARIS

ORDRE DES AVOCATS DE PARIS

COMMISSION OUVERTE
LES NOUVEAUX MÉTIERS DU DROIT



Severine Audoubert
Responsable
Avocat à la cour

Oriana Labruyère
Intervenante
Avocat à la cour

Nathalie Chiche
Intervenante
Avocat à la cour

LES INTERVENANTS

Severine Audoubert
Responsable

Avocat à la cour

Membre du Conseil National des Barreaux CNB, Vice Présidente de la Commission Communication Institutionnelle, Membre de la Commission Prospective et Innovation, Membre de la Commission Règles et Usages

Présidente de la Commission Ouverte Nouveaux Métiers Barreau de Paris

Fondatrice de myentrepreneurbox.com

LES INTERVENANTS

Oriana Labruyère
Intervenante

Avocat à la cour

Oriana Labruyère a fondé son cabinet en droit du numérique et assure des missions de DPO externalisé pour des organisations de toutes tailles.

Elle traite les enjeux liés à la conformité dans divers environnements allant de la PME à la multinationale, en France et à l'international. elle a acquis son expérience au sein de divers cabinets et d'entreprises en France et à l'international.

Oriana dispose d'une double compétence en droit et gestion de projet lui permettant de mettre son expertise juridique au service des entreprises. Elle s'attache à fournir des réponses concrètes aux contraintes opérationnelles et juridiques.

Elle est aussi élue municipale et réalise un podcast « La Robe Numérique » qui met en lumière des solutions de la tech française ou européenne et répond aux enjeux juridiques modernes.

LES INTERVENANTS

LE CLUB DPO

Nathalie Chiche
Avocate au Barreau de Paris & DPO externe

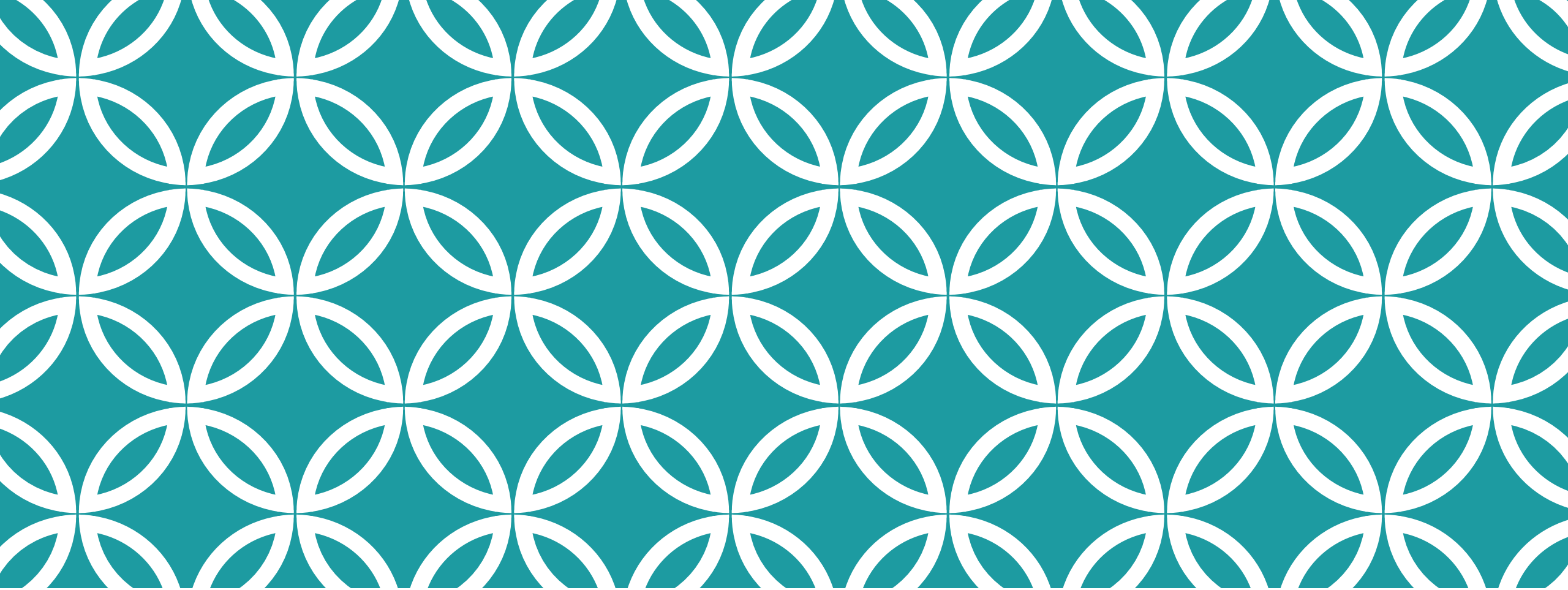
Présidente du Club DPO Association du Barreau de Paris

Passionnée de la protection des données et titulaire d'un Diplôme Universitaire Data Protection Officer, elle exerce depuis plus de 7 ans la fonction de Data Protection Officer et elle a été désignée à la CNIL.
Elle est à l'initiative de la création du Certificat DPO de l'Université de Paris Dauphine - Tunis et a enseigné au sein du Diplôme Universitaire DPO (Data Protection Officer) de Paris Dauphine et au sein du Master spécialisé Data Protection Management (MS DPM) de l'Institut Telecom Business School.

Elle a également à cœur d'accompagner les entreprises en matière de protection des données à caractère personnel (formation et sensibilisation, audit et mise en conformité, politique et gouvernance d'entreprise, assistance aux délégués à la protection des données, maintien en conformité réglementaire,...).

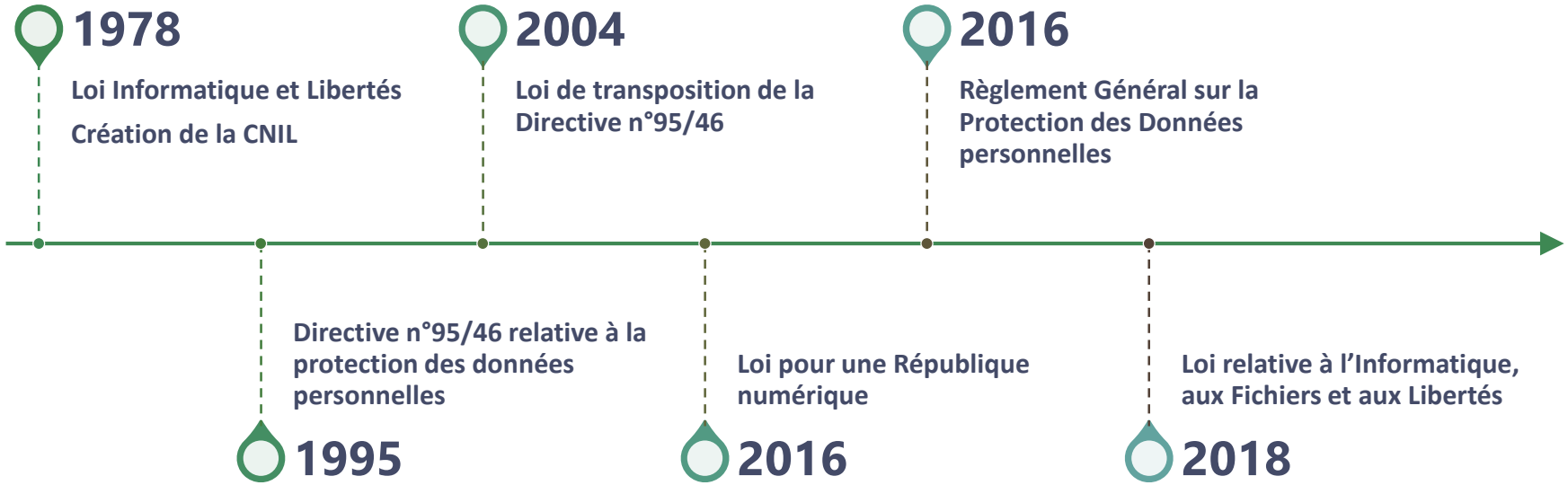
Elle est fondatrice et Présidente du Club DPO et membre de l'Association Française des Correspondants à la protection des Données à caractère Personnel regroupe les Délégués à la protection des données (DPO) et participe aux groupes de travail et livres blancs de ces organisations.

Elle a participé au « Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises » publié en 2018 par la Banque Publique d'investissement (BPI) et la Commission Nationale Informatique et Libertés (CNIL).



INTRO

PETIT HISTORIQUE



Chiffres clés des sanctions CNIL en 2022

15 000

Plaintes reçues

22

Sanctions prononcées

175 000€

Montant de la sanction publique la plus faible

300

Contrôles réalisés par an

4

Sanctions selon la procédure simplifiée

60 000 000€

Montant de la sanction publique la plus importante

100 927 900 €

Quels manquements sanctionnés en 2022 ?

Manquements	Occurrences
Consentement	8
Sécurité	6
Gestion des droits	6
Transparence	6
Durée de conservation	3
Minimisation	1
Sous-traitance	1
Absence de base juridique	1
Absence de coopération	1
Privacy by default	1
Absence d'AIPD	1
Absence de documentation des violations de données	1

Les montants estimés des amendes en Europe

2018

458 000 euros

2019

73 millions d’euros

2020

171 millions d’euros

2021

1,1 milliard d’euros

2022

841 millions d’euros

LA ROBE NUMÉRIQUE

Les montants estimés des amendes en France

2018

0 euros

2019

51,1 millions d’euros

2020

3,3 millions d’euros

2021

3,7 millions d’euros

2022

25,2 millions d’euros

LA ROBE NUMÉRIQUE

LES AVOCATS ?

L'USINEDIGITALE

Start-up Cybersécurité Réglementation Intelligence artificielle AR/VR Mobilité Plus

DONNÉES PERSONNELLES \ CYBERSÉCURITÉ \ ETATS-UNIS

Des hackers réclament 42 millions de dollars à un cabinet d'avocats pour ne pas divulguer les données de célébrités

Le groupe de pirates informatiques qui se cache derrière le ransomware REvil affirme être en possession de 756 Go de données appartenant à de célèbres clients de Grubman Shire Meiselas & Sacks. Ce cabinet d'avocats new-yorkais s'est vu réclamer une rançon record de 42 millions de dollars pour obtenir une clé de déchiffrement, mais assure à date ne pas vouloir la verser. Les hackers menacent de divulguer une partie des fichiers en ligne.

Arthur Le Denn
19 mai 2020 | 12h25

2 min. de lecture

Réagir →

Capital

Accueil > Crypto

Ledger : les victimes de la fuite de données entament une action en justice

BITCOIN SUIVRE CE SUJET

LA TRIBUNE

ÉCONOMIE BOURSE ENTREPRISES & FINANCE TECH IDÉES RÉGIONS T LA REVUE

Cybercriminalité : la soi-disant fuite du ministère de la Justice concerne en fait un cabinet d'avocats

Fausse alerte. Les cybercriminels de Lockbit, qui prétendaient détenir des données du ministère de la Justice et menaçaient de les publier, bluffaient. En réalité, leur butin ne contient que des documents issus d'un cabinet d'avocat, et notamment de ses ressources humaines. Un véritable problème pour les personnes concernées, mais l'incident est finalement d'une ampleur moindre qu'annoncée.

LT Réservé aux abonnés

Powered by ETX Studio

00:00/00:00

François Manens
02 Févr 2022, 12:41

SUDOUEST.FR JEUX LES I

Ecouter cet article Emeutes : les données personnelles d'un millier de juges et avocats publiées 00:00

Un groupe de hackers a publié, en réponse aux émeutes, un document contenant des données personnelles de 1 120 magistrats et avocats sur un canal Telegram

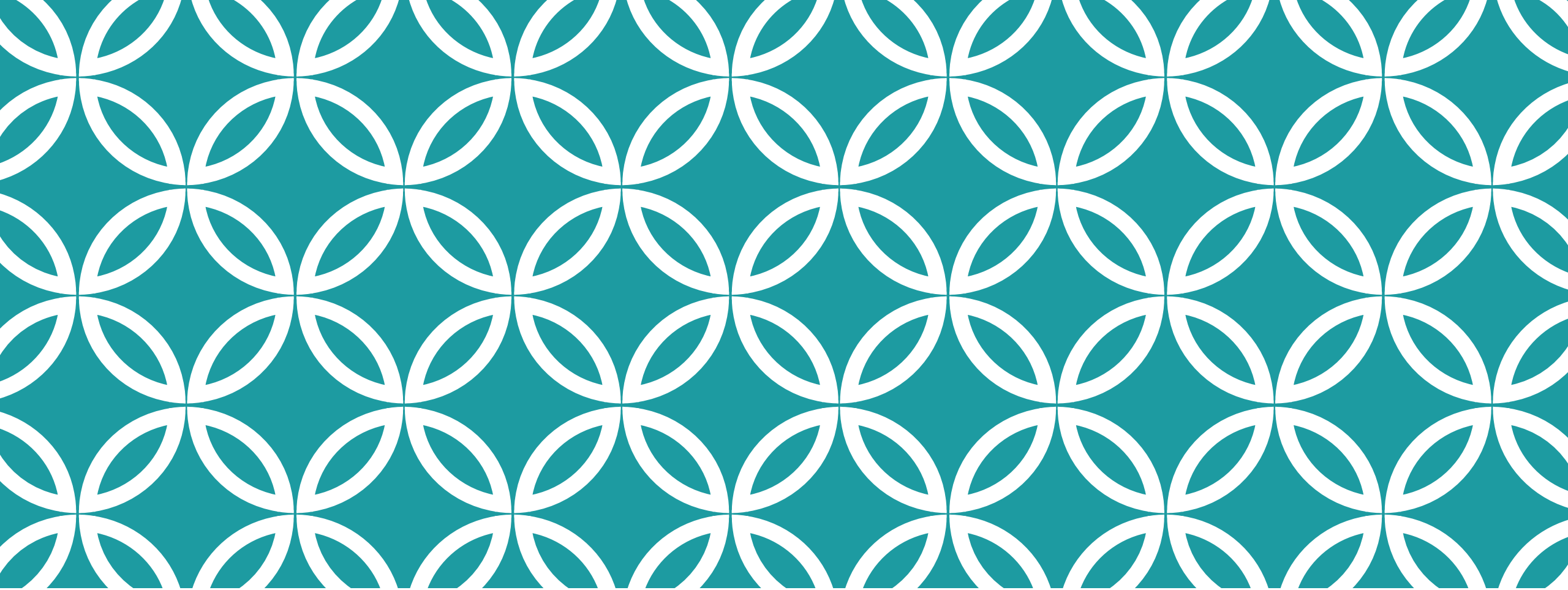
C'est un groupe nommé Kromsec qui revendique cette fuite de données. Celle-ci concerne du personnel juridique français, selon Numérama. Le document en ligne contient notamment des noms associés à des mails professionnels, des numéros, des adresses et des IBAN. Selon « le Monde », le groupe de hackers affirme que ces informations proviennent d'un piratage,

ici PAR FRANCE BLEU ET FRANCE 3 | Le média de la vie locale

Un Strasbourgeois lance l'alerte sur une fuite de données à l'Urssaf, près de 700 Alsaciens concernés

C'est un Strasbourgeois qui a donné l'alerte. Une erreur informatique survenue ce lundi est à l'origine d'une importante fuite de données personnelles à l'Urssaf. Des milliers de travailleurs indépendants sont concernés en France, parmi eux près de 700 Alsaciens.

LA ROBE NUMÉRIQUE



RGPD : QUESA QUO ?

LE TRAITEMENT DE DONNÉES PERSONNELLES

Le **RGPD** est applicable aux *traitements de données à caractère personnel* automatisés en tout ou en partie, ou non automatisés de données à caractère personnel (**article 2 du RGPD**).

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des **données personnelles**, quel que soit le procédé utilisé.

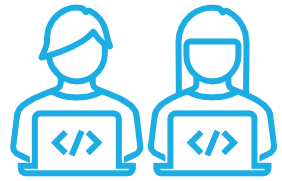
Toute information relative à une **personne physique** **identifiée** ou **identifiable** (personne concernée) de manière **directe** ou **indirecte** (article 4.1 RGPD)

LA ROBE NUMÉRIQUE

LES ACTIVITÉS : TOUTES CONCERNÉES

Judiciaire ou conseil : même régime

Exercice individuel ou non, avec les collaborateurs



Dans tous les services de l'avocat : prestataires, hébergement, boite mail …

LA ROBE NUMÉRIQUE

LE FONDEMENT DU TRAITEMENT

Respect obligation légale

Dans le cadre de la gestion du personnel tel que les obligations liées à la déclaration sociale nominative (DSN) ou encore à la tenue d'un registre unique du personnel.

Consentement

Il est nécessaire pour encadrer les traitements n'ayant pas d'autres bases légales possibles.

Mesures contractuelles ou précontractuelles

La conclusion du contrat entre l'entreprise et ses clients

Exécution d'une mission d'intérêt public

Spécifique pour les missions d'intérêt public (par exemple les missions de la CNIL)

Intérêt légitime de l'organisme

La sécurité du système informatique, l'organisation du travail interne, la mise en place de formations.

Sauvegarde des intérêts vitaux

Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers.

LES PRINCIPES (1/2)

Une collecte loyale et transparente

→ **Gage de confiance** entre le responsable de traitement, les personnes dont les données sont traitées ainsi que l'autorité de contrôle.

→ Toute information se rapportant aux traitements de données personnelles doit être communiquée sous une **forme intelligible.**

Une finalité et des sous-finalités identifiées

→ On ne peut collecter et traiter des données que dans un but **légitime, légal et précis**.

→ Lorsqu'une finalité est identifiée pour un traitement de données, il n'est pas possible d'**utiliser ces mêmes données pour une autre finalité** sans le consentement des individus concernés.

Une collecte et un traitement proportionné

→ Les activités de traitement doivent être strictement limitées à ce qui est **nécessaire à l'accomplissement des finalités du traitement.**

→ **Principe d'interdiction** : données sensibles, données pénales, données particulières.

Une responsabilité encadrée

→Les **acteurs du traitement de données doivent être clairement identifiés** afin de définir leurs responsabilités respectives (relations de sous-traitance ou de co-traitance).

LES PRINCIPES (2/2)

Une conservation limitée

→ La conservation des données personnelles est **strictement limitée dans le temps**. Des durées de conservation doivent être établies pour chaque type de données traitées.

→ La durée de conservation ne doit **pas excédée** celle nécessaire à la finalité poursuivie.

Des individus protégés

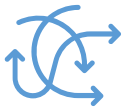
→ Les individus dont les données sont collectées et traitées possèdent des **droits relatifs à ces données** (information, opposabilité, portabilité, etc.)

→ Des mesures doivent être mises en place pour qu'ils puissent **exercer** ces droits et **répondre** à leurs demandes.

Une sécurisation renforcée

→ Principe général de sécurisation des traitements et des données personnelles.

→ Mise en place d'une **politique de sécurité** et de toutes **mesures organisationnelles et techniques** adéquates (pseudonymisation, chiffrement…)



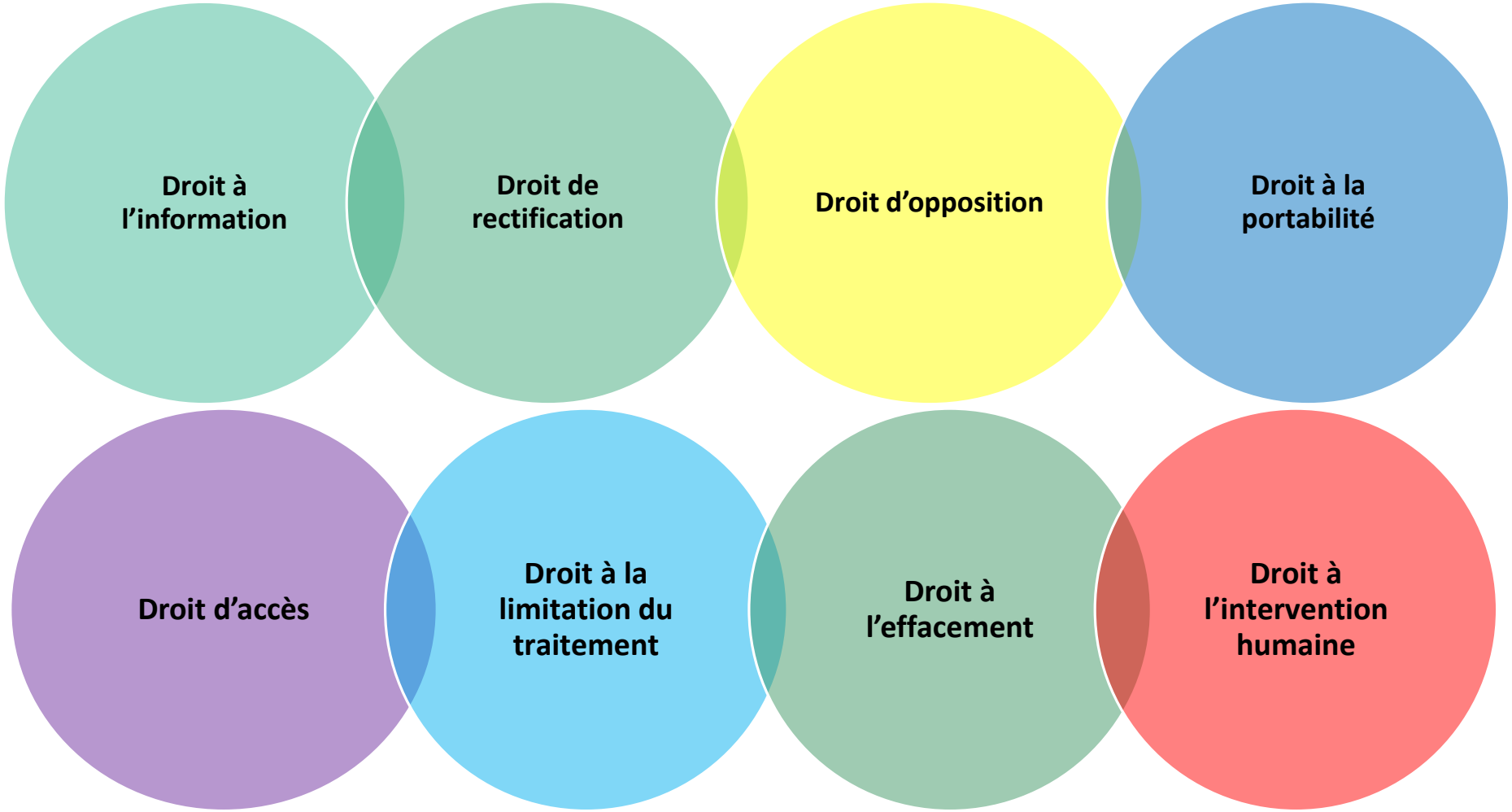
Une traçabilité des données

→ L'ensemble des traitements sur les données doit être **répertorié au sein d'un registre** à des fins de contrôle interne et externe et les risques y afférents sont analysés.

→ Permet l'identification des **flux de données hors UE** et la formalisation des registres de suivi des **demandes de droit et des incidents**.

LA ROBE NUMÉRIQUE

LES DROITS DES PERSONNES



LA ROBE NUMÉRIQUE

ZOOM : CONSERVATION LIMITÉE DES DONNÉES

PRINCIPE

La conservation des données personnelles est **strictement limitée dans le temps**. Des durées de conservation doivent être établies pour chaque type de données traitées.

INTERDICTION

De conserver des données pour une **durée excédant celle nécessaire à la finalité** poursuivie.

EXCEPTION

Statistiques et recherche scientifique.

- Sanctions pénales (article 226-20 code pénal)
- Sanctions administratives rendues par la CNIL (article 83 RGPD)

LA ROBE NUMÉRIQUE

Illustrations des sanctions

Les données collectées dans la base nationale des identifiants élèves pendant une **durée totale de 35 ans** est **excessive**. (CE, 19 juillet 2010, M. Fristot et a.)

La société ne respectait pas les durées de conservation définies dans son référentiel, et conservait les données personnelles de ses prospects et clients sur des **durées excessives**. (CNIL, 22 juillet 2021, AG2R La Mondiale)

La **conservation de fichier d'évaluation d'agent** pendant **plus de 3 ans** après la commission d'avancement était excessive. (CNIL, 29 octobre 2021, RATP)

Il est possible de conserver les données pour des durées plus longues pour des **finalités de recherche**, mais il est alors nécessaire de mettre en œuvre des **mesures techniques et organisationnelles appropriées** pour garantir les droits et libertés des personnes concernées. (31 janvier 2022)

ZOOM : RESPONSABILITÉ ENCADRÉE

PRINCIPE

- Les acteurs du traitement de données doivent être clairement identifiés afin de définir leurs responsabilités respectives (relations de sous-traitance ou de co-traitance)

COMMENT ?

- Identification des acteurs
- Mise à jour contractuelle
- Contrôle de conformité des tiers (en particulier des sous-traitants)

Illustrations des sanctions

Les contrats conclus par la société avec ses prestataires **sans qu'ils contiennent de clauses, ni de mentions** ne respectent pas les obligations de l'article 28-3 du RGPD. (CNIL, 28 décembre 2021, Sté Slimpay).

Le contrat conclu entre la société et son sous-traitant ne contient pas de clauses prévoyant les engagements de ce dernier. (CNIL, 7 décembre 2020, Sté Performeclic)

A été sanctionné par la CNIL un responsable de traitement et son sous-traitant pour ne pas avoir pris des mesures de sécurité satisfaisantes pour faire face à des attaques par bourrage d'identifiants sur le site web du responsable de traitement. (CNIL, 27 janvier 2021)

SANCTION CIVILE / SANCTION PÉNALE

RGPD

Article 82 du RGPD :

« *Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du [RGPD] a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.* »

Article 84 du RGPD :

« Les Etats membres peuvent mettre en place des sanctions supplémentaires en cas de violation du RGPD ».

Code pénal

Article 226-16 et suivants du Code pénal :

Les sanctions pénales peuvent aller **jusqu'à 5 ans d'emprisonnement** et **300 000 euros d'amende.**

Exemple de sanctions dans le secteur juridique

Le 8 septembre 2022, la formation restreinte de la CNIL a prononcé une sanction de **250 000 euros** à l'encontre du GIE **INFOGREFFE** pour avoir manqué à plusieurs obligations du RGPD en matière de durées de conservation et de sécurité des données personnelles.

SANCTION ADMINISTRATIVE

Procédure de sanction ordinaire

Le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial. Ces sanctions peuvent être rendues **publiques.**

La formation restreinte de la CNIL peut:

- Prononcer un rappel à l'ordre;
- Enjoindre de conformer le traitement;
- Limiter temporairement ou définitivement un traitement;
- Suspendre les flux de données;
- Ordonner de satisfaire les demandes d'exercice des droits des personnes;
- Prononcer une amende administrative.

Procédure de sanction simplifiée

Une procédure de sanction simplifiée ne peut être engagée que dans l'hypothèse d'un **dossier peu complexe** ou de **faible gravité**.
Les **sanctions** susceptibles d'être prononcées dans la procédure simplifiée sont **moins nombreuses et moins sévères** que celles encourues dans la procédure ordinaire. Elles ne peuvent par ailleurs **jamais être rendues publiques.**

Le président de la formation restreinte peut :

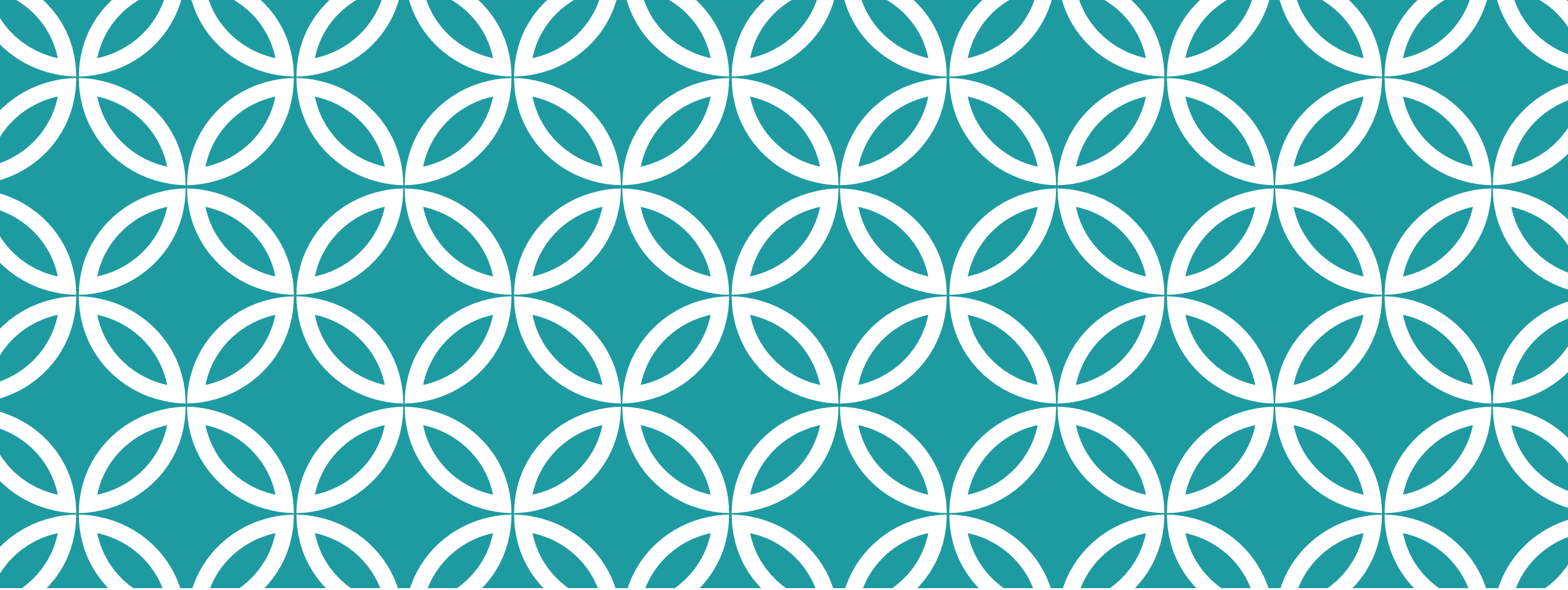
- Prononcer un rappel à l'ordre;
- Enjoindre de mettre le traitement en conformité, y compris sous astreinte d'un montant maximal de 100 euros par jour de retard;
- Prononcer une amende administrative d'un montant maximal de 20 000 euros.

Les chiffres en 2022

21 sanctions pour un total de **101 277 900 euros**

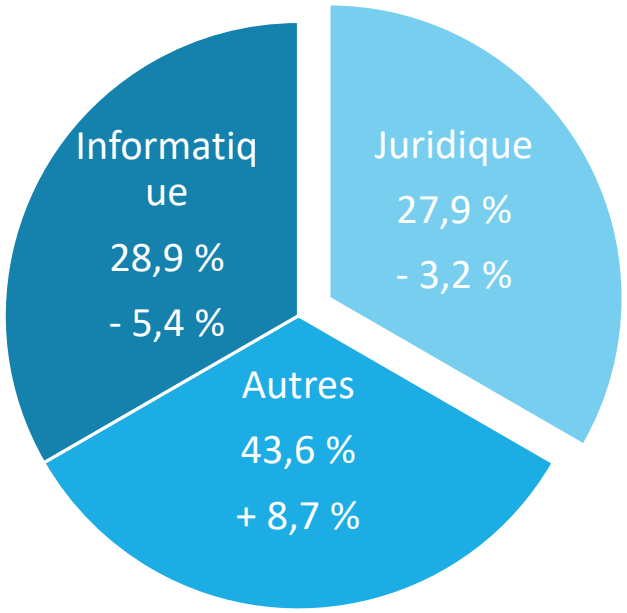
projets de sanctions européens examinés par la CNIL

LA ROBE NUMÉRIQUE



CRÉATION DE L'AVOCAT DPO

L'AVOCAT-DPO : LE CONSTAT



Un bon DPO apporte sa connaissance spécifique des textes et règlements européens.

L'avocat-DPO apportera en plus son expertise juridique, de la défense, du conseil continu et d'un encadrement juridique en cas de contrôle.

La fonction de l'avocat l'habitue à veiller à la protection des libertés publiques et individuelles. Par conséquent, il peut jouer un rôle essentiel dans la protection des données personnelles.

LE CADRE DÉONTOLOGIQUE DE LA FONCTION AVOCAT-DPO

Ajout de la possibilité d'être DPO : une décision du 27 janvier 2017 (prise suite à la délibération du 9 décembre 2016, DCN n°2016-002, AG du 9 décembre 2016), le CNB a modifié les dispositions de l'article 6 du Règlement intérieur national de la profession d'avocat (RIN) afin de tenir compte de la possibilité, désormais offertes aux avocats d'exercer les fonctions de délégué à la protection des données.

6.4. du RIN

L'avocat qui souhaite exercer en tant que DPO doit informer le Bâtonnier par une déclaration écrite.

Mail, courrier postal : aucun formalisme particulier n'est requis.

LA RÈGLEMENTATION DES CONFLITS D'INTÉRÊTS

L'article 6.3.3.

du RIN

« L'avocat Délégué à la Protection des Données doit mettre un terme à sa mission s'il estime ne pas pouvoir l'exercer, après avoir préalablement informé et effectué les démarches nécessaires auprès de la personne responsable des traitements ; en aucun cas il ne peut dénoncer son client. L'avocat Délégué à la Protection des Données doit refuser de représenter toute personne ou organisme pour lesquels il exerce ou a exercé la mission de correspondant à la protection des données à caractère personnel (CIL) ou de Délégué à la Protection des Données dans le cadre de procédures administratives ou judiciaires mettant en cause le responsable des traitements ».

L'enjeu de l'indépendance est ici primordial dans la pratique du métier d'avocat et se retrouve dans toutes les étapes de la relation client et ce dès la négociation de la convention d'honoraires : forfait, durée …

INTERDICTION DE LA DOUBLE FONCTION EN CAS DE POURSUITE DU RT

L'Avocat-DPO ne peut pas défendre ou conseiller le client poursuivit pour un traitement qu'il met en œuvre.

- **Principe :** L'avocat-DPO ne peut pas défendre, ou assister, le Responsable du traitement lorsque ce dernier voit sa responsabilité civile engagée du fait d'une violation de la protection des données personnelles.
  Exemple : détournement de finalités, non-respect des règles en matière de durées de conservation, collecte illégale de données personnelles sensibles, etc.

- **L'enjeu :** L'avocat DPO ne doit pas se retrouver en conflit entre sa responsabilité d'avocat et celle de son client.

LE CADRE DÉONTOLOGIQUE : ENTRE OBLIGATION ET PRINCIPES

UNE OBLIGATION DE LOYAUTÉ À SON RESPONSABLE DU TRAITEMENT VS INDEPENDANCE ET IMPARTIALITE

- L'obligation de loyauté est inhérente à la profession d'avocat est n'est qu'un rappel de l'article 4.1 du RIN.
- Cependant, le DPO au regard de son positionnement dans l'organisation peut être amené à constater des pratiques répréhensibles consistant en des violations caractérisées et délibérées des règles en matière de protection des données.
- Conséquence : le secret professionnel protège le client mais l'avocat doit démissionner.
- Ainsi, l'obligation d'indépendance et d'impartialité auquel est tenu le délégué à la protection des données ne signifie pas que ce dernier ne doit pas pour autant être loyal à son Responsable du traitement.

En pratique : le cas du traitement illégal

L'AVOCAT EST UN DPO AUGMENTÉ

- **Accompagnement et conseil du Responsable de Traitement :** Conseil et recommandation auprès de la direction : rédaction de note, mise en place de support de présentation.

- **Mise en œuvre de la méthode de Privacy by design / by default :** Conseil pour prendre en compte la protection des données personnelles dans l'ensemble des processus de l'entreprise : revue ou rédaction de note d'organisation spécifique.

- **Audit et suivi de la conformité au quotidien :** Gestion des demandes des tiers (demandes de droits ou demandes liées aux contrats) : revue contractuelle et analyse des zones de risque.

- **Gestion de crise :** Préparation à la gestion de crise en amont et lors de la crise : établissement des éléments, rédaction des éléments de gouvernance, analyse et note sur la situation, aide à l'évaluation et à la décision.

SE LANCER EN TANT QUE DPO

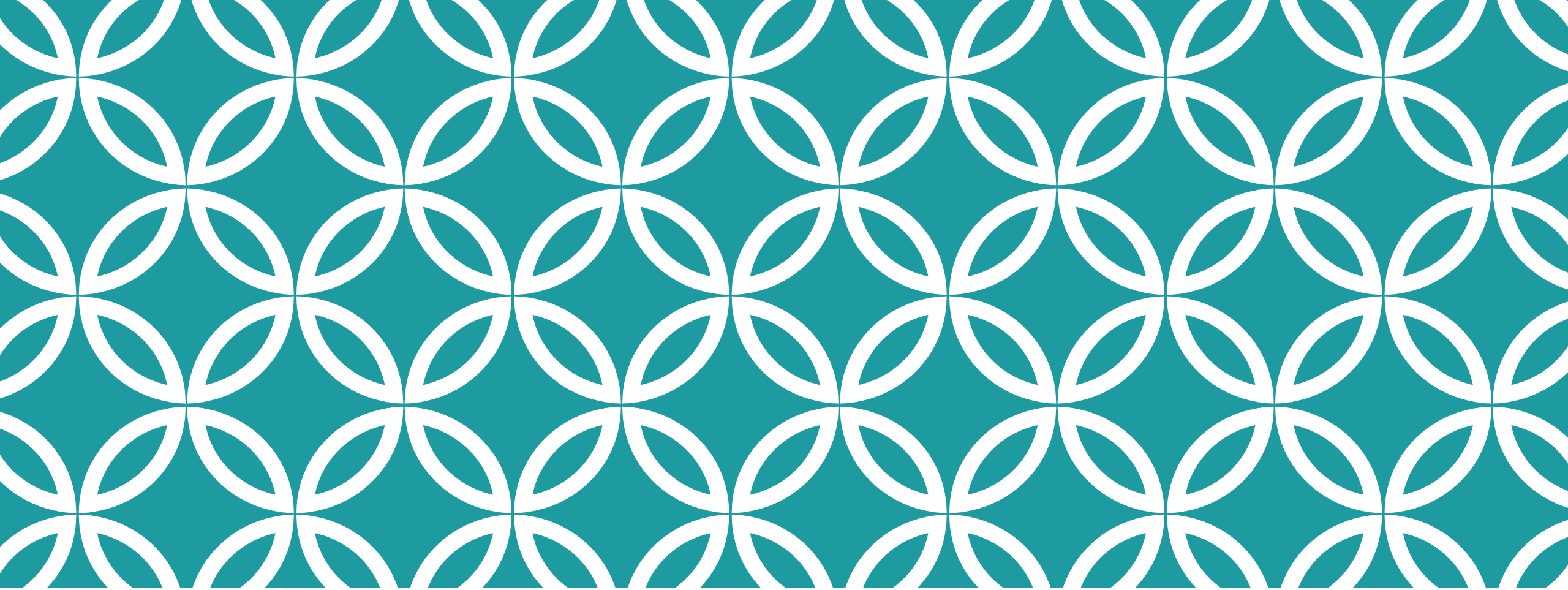
Identifier le besoin chez le client

Rédiger sa proposition d'accompagnement

Connaitre les enjeux déontologiques du DPO

Gérer la prise de poste

Identifier les outils



BOITE À OUTILS

LA BOITE À OUTILS

Le Guide Pratique : les avocats et le RGPD, éd. Mai 2023 par le CNB, Barreau de Paris, la Conférence des Bâtonniers

Les outils de la conformité produit par la CNIL :
- registre de traitement
- mention d'information
- l'analyse d'impact relative à la protection des données (AIPD)
- le transfert de données hors UE

Le Club des DPO :

PRÉSENTATION DU CLUB DPO

LE CLUB DPO

LE CLUB DPO

Le réseau privé d'experts (par cooptation) en protection des données

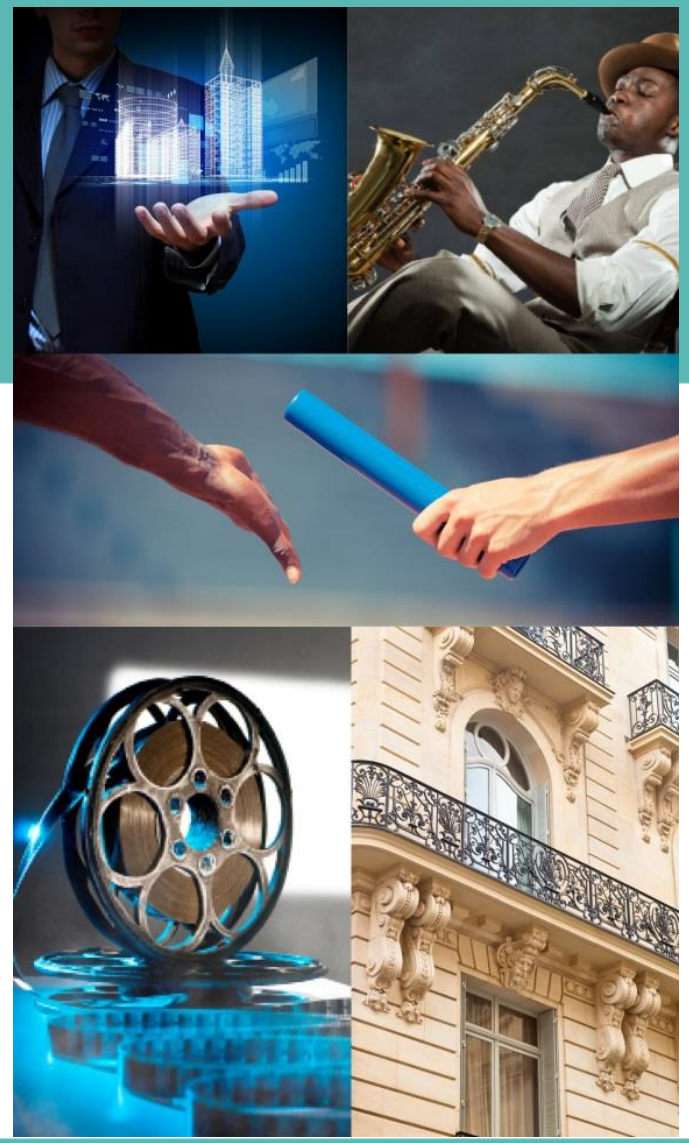
Le Club DPO rassemble des experts de la protection des données (Avocats & DPO) justifiant d'un minimum de 5 années d'expérience professionnelle et intervenant dans tous les secteurs d'activités et partout en France.

Ce réseau vise à favoriser les échanges et les partages d'expériences entre les DPO du Club. Les adhérents du Club DPO sont force de proposition dans l'exercice de leur métier et ils rendront compte régulièrement de leurs réflexions et avancées à tout le groupe.

Pour nous joindre **contact@clubdpo.fr**

AVOCATS
BARREAU
• PARIS

ORDRE DES AVOCATS DE PARIS



MERCI A TOUS