NEWSLETTER RGPD

NUMÉRO 36 ● OCTOBRE 2021

ACTUALITE DU CABINET

FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ».

Le cabinet organise régulièrement des programmes de formation visant à la préparation des apprenants à l'examen de certification « DPO ».

Retrouvez notre programme à la fin de notre newsletter. **P.15**

SOMMAIRE

LE LIVRE BLANC DE LA CNIL SUR LES DONNEES ET LES MOYENS DE PAIEMENT

LA CNIL A PUBLIE UN LIVRE BLANC INTITULE « QUAND LA CONFIANCE PAIE : LES MOYENS DE PAIEMENT D'AUJOURD'HUI ET DE DEMAIN AU DEFI DE LA PROTECTION DES DONNEES », AFIN « D'ECLAIRER LE PUBLIC, D'ACCOMPAGNER LES PROFESSIONNELS ET D'ANTICIPER LES TRANSFORMATIONS A VENIR ».

La CNIL, dressant le constat de transformations économiques (le paiement sans contact, le recul de l'usage des espèces, les transferts entre particuliers) induisant des enjeux pour la vie privée, vient de publier un livre blanc sur les données et les moyens de paiement.

L'objectif de ce document est d'« *apporter des éclairages sur les principaux enjeux économiques, juridiques et sociétaux des données et des moyens de paiement* ».

La CNIL indique, ainsi, dans ce document, que les périodes de confinement ont entrainé un recul très net des moyens de paiement impliquant un contact physique, ainsi qu'une croissance du sans contact (+37% entre 2020 et 2019) et des paiements en ligne (+13% sur la même période). L'autorité de contrôle ajoute toutefois que, si l'usage de la monnaie électronique est en hausse (+22.6 % entre 2019 et 2020), elle reste marginale (1% des paiements en termes de volume et de valeur).

Pour la CNIL, les données de paiement peuvent comporter des enjeux particuliers, notamment dans la mesure où elles sont susceptibles de « *permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* ».

Une autre spécificité des données de paiement est qu'elles peuvent, dans certains cas, concerner des tiers, tels que des personnes bénéficiaires d'une transaction.

Par ailleurs, « *les opérations de paiement dans leur ensemble peuvent occasionner un traitement de données sensibles au sens du RGPD, par exemple si une méthode d'authentification biométrique est utilisée* ».
Enfin, la CNIL rappelle que le CEPD qualifie certaines d'entre elles de « *données hautement personnelles* » lorsqu'elles révèlent une géolocalisation ou peuvent être utilisées pour commettre des fraudes au paiement : c'est le cas des numéros de carte bancaire et autres identifiants de paiement par exemple. Ces dernières données concentrent évidemment des enjeux très élevés en termes de sécurité.
Huit messages clés sont développés dans ce document :

- la préservation de l'anonymat des paiements, de l'usage des espèces et du libre choix des moyens de paiement ;

- l'importance d'une protection de la confidentialité des transactions dès la conception dans le projet en cours d'euro numérique, lancé par la Banque centrale européenne en juillet ;

- l'attention prospective à porter au paiement mobile, qui a un potentiel de développement considérable ;

- l'intérêt pour les acteurs innovants de faire de leur conformité au RGPD un atout de confiance pour les clients amenés à confier leurs données pour de nouveaux usages ;

- les grands points d'application du RGPD sur lesquels la CNIL souhaite apporter de la sécurité juridique ;

- l'importance de la sécurité des données de paiement, avec des travaux sur la « tokenisation » de ces données en tant que bonne pratique ;

- un questionnement sur la localisation des données de paiement en Europe, comme contribution au débat en cours sur la souveraineté numérique européenne ;

- des recommandations pour le futur réseau de carte bancaire européen en cours de création, EPI (« European Payments Initiative »).

Ce livre blanc n'est, pour la CNIL, qu'une « *première étape du dialogue* » qu'elle souhaite ouvrir avec les parties prenantes (grand public, professionnels, groupes d'intérêt, chercheurs, régulateurs, etc.) sur le sujet des paiements. Une consultation publique en ligne a été ouverte, visant à recueillir les réactions suite à la publication de ce livre blanc, ainsi que les positions, témoignages et besoins de toutes les parties prenantes.

LA CNIL MET EN DEMEURE LA SOCIETE FRANCETEST POUR SECURISATION INSUFFISANTE DES DONNEES DE SANTE

Par deux délibérations en date des 4 et 11 octobre 2021 (accessibles ici et ici), la CNIL a rendu publique sa mise en demeure de la société FRANCETEST en raison de la sécurisation insuffisante des données de santé.

La société FRANCETEST développe un service à destination des pharmacies qui effectuent des tests antigéniques au COVID-19.

Elle met notamment en œuvre le site internet www.francetest.fr qui permet :

- de simplifier la collecte des données personnelles des patients testés ; et
- l'acheminement des données collectées vers le système d'information national de dépistage (traitement mis en œuvre par le Ministère des solidarités et de la santé, centralisant les résultats de ces tests (le « SI-DEP »).

A ce titre, la société FRANCETEST est en relation d'affaires avec 350 pharmacies et sa base de données comporte des données relatives à plus de 400.000 tests, concernant environ 387.000 personnes uniques.

Parmi les données collectées figurent : le nom, le prénom, l'adresse email, la date de naissance, le numéro de téléphone, le résultat du test (positif ou négatif) et également le NIR des personnes testées.

Le 27 août 2021, la CNIL a été saisie d'un signalement anonyme faisant état d'une faille de sécurité affectant le site internet de la société FRANCETEST.

A l'issue de vérifications en ligne, une vulnérabilité a été constatée en raison d'un défaut de configuration du serveur web entrainant la libre accessibilité de toutes les données personnelles renseignées par les personnes lors de la réalisation d'un test.

La CNIL a effectué un contrôle sur place dans les locaux de la société FRANCETEST afin de vérifier la conformité des traitements de données personnelles mis en œuvre par cette dernière avec le RGPD et la Loi Informatique et Libertés.

Après avoir qualifié la société FRANCETEST de sous-traitant, la CNIL a retenu un manquement à l'article 32 du RGPD.

1. Sur la qualification de sous-traitant de la société FRANCETEST

Selon l'article 4, paragraphe 8 du RGPD, le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou autre organisme qui traite les données à caractère personnel pour le compte du responsable du traitement ».

En l'espèce, la CNIL a estimé que la société FRANCETEST doit être regardée comme sous-traitante des pharmacies car « d'une part, [la société FRANCETEST] ne fait que mettre à disposition les outils, notamment informatiques, choisis par les pharmacies pour faciliter la mise en œuvre du traitement et, d'autre part, agit uniquement au nom et sous la responsabilité des pharmacies ».

2. Sur le manquement à l'article 32 du RGPD

L'article 32 du RGPD impose de « mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».
Aussi, aux termes du considérant 75 du RGPD, le traitement qui porte sur des données de santé doit bénéficier de mesures de sécurité renforcées.
A ce titre, l'article L.1111-8 du Code de la santé publique prévoit que les données de santé doivent être hébergées par un hébergeur disposant d'un agrément « HDS » délivré par le Ministère des solidarités et de la santé.

En l'espèce, la CNIL a retenu un manquement à l'article 32 du RGPD en raison d'insuffisances en termes de sécurité des données puisque :

- le prestataire hébergeant des données de santé ne disposait pas de l'agrément HDS ;
- les processus d'authentification étaient insuffisamment robustes ;
- la fonction de hachage utilisée était faible ; et
- la journalisation des activités des serveurs du service FRANCETEST était lacunaire.

Tirant les conséquences de ce manquement, la CNIL a mis en demeure la société FRANCETEST de prendre toute mesure pour garantir la sécurité et la confidentialité des données, dans un délai de 2 mois à compter de la notification de la mise en demeure.

En outre, la CNIL a estimé que la publicité de la mise en demeure était justifiée en raison de la sensibilité des données traitées et de la nécessité d'informer les personnes concernées par les traitements en cause ainsi que les organismes ayant recours aux services de la société FRANCETEST.

CONDAMNATION DE SKY ITALIA A UNE AMENDE DE 3.296.326 EUROS POUR PROSPECTION TELEPHONIQUE ILLICITE

DERRIENNIC ASSOCIÉS
CONDAMNATION DE SKY ITALIA À UNE AMENDE DE 3.296.326 EUROS POUR PROSPECTION TÉLÉPHONIQUE ILLICITE

L'autorité de contrôle italienne compétente en matière de protection des données a prononcé une sanction à l'encontre d'une société qui avait procédé à des opérations illicites de prospection téléphonique.

L'autorité de contrôle italienne, la « GPDP », a reçu un nombre important de plaintes l'informant que la société Sky Italia, éditrice d'un service de bouquet de télévision par satellite, procédait à des appels téléphoniques de prospection, d'une part, sans délivrer aux personnes prospectées une information quant aux traitements de données réalisés et, d'autre part, sans recueillir son consentement.

Sky Italia procédait en effet à des opérations de prospection téléphonique, en utilisant des données transmises par des prestataires, dont le contrat prévoyait :

(i) que ces prestataires sélectionneraient, dans leur propre base de données, les coordonnées de personnes ayant consenti au traitement de leurs données à des fins de prospection par des tiers ;

(ii) que ces prestataires adresseraient des sollicitations commerciales aux personnes dont les données ont ainsi été sélectionnées, pour le compte de Sky Italia.

Sky Italia se voyait également communiquée des données de la part de ses prestataires, qu'elle utilisait afin de procéder elle-même à des opérations de prospection téléphonique.

Sky Italia considérait que ses prestataires étaient responsables du traitement et étaient donc en charge de veiller à ce que les personnes concernées soient informées du traitement et aient donné leur consentement aux opérations de prospection commerciale envisagées.

En conséquence, lorsque Sky Italia contactait les personnes concernées aux fins de prospection, elle ne leur délivrait pas d'information quant au traitement de leurs données à caractère personnel.

En pratique, dans un certain nombre de cas, les personnes faisant l'objet de sollicitations commerciales n'avaient donné leur consentement que s'agissant du transfert de leurs données à Sky Italia, mais pas pour que Sky Italia procède à des opérations de prospection avec leurs données à caractère personnel.

Pour l'autorité de contrôle, le consentement donné par les personnes concernées aux prestataires concernait la communication des données à des tiers et non la possibilité pour Sky Italia d'utiliser ces données à des fins promotionnelles. L'autorité italienne précise que Sky Italia aurait dû vérifier que ce consentement, aux fins de prospection, était bien collecté par elle ou par ses partenaires.

Afin de mener à bien ses activités de télémarketing, Sky Italia, au début de chaque appel téléphonique, aurait dû fournir à la personne prospectée une information quant au traitement de ses données, incluant la source desdites données, et, seulement après avoir obtenu le consentement, réaliser l'opération de prospection commerciale.

Enfin, Sky Italia aurait dû contrôler l'activité de ses prestataires en charge des opérations de prospection, ceux-ci devant, selon l'autorité de contrôle italienne, être qualifiés de sous-traitant, y compris s'agissant de leur mission de sélection des données à caractère personnel parmi celles figurant dans leurs propres bases de données.

L'autorité italienne a enjoint à Sky Italia de corriger l'ensemble de ces manquements et l'a condamné à une amende d'un montant de 3.296.326 euros.

Lien vers la décision :

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9706389

ACTUALITE EUROPEENNE :

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITES NATIONALES DE CONTROLE

Sanction du propriétaire d'un bar pour avoir détourné la finalité de ses caméras de vidéosurveillance

AEPD (ESPAGNE), 28 SEPTEMBRE 2021

Le 20 juin 2014, le client d'un bar de la ville d'Almeria en Espagne a subi une chute accidentelle au sein de l'établissement.

Enregistrée par les caméras de vidéosurveillance, la chute a été diffusée par le propriétaire du bar sur un groupe WhatsApp, puis dans un journal numérique local.

Le client, estimant que la vidéo porte atteinte à son honneur et à son image, a déposé une plainte auprès de l'autorité de contrôle espagnole.

L'autorité de contrôle, après avoir rappelé que l'image d'une personne est une donnée personnelle et que la finalité d'un système de vidéosurveillance est de garantir la sécurité des biens et des personnes, a estimé que la publication de la vidéo viole le principe de limitation des finalités posé à l'article 5(1)b du RGPD en ce que les images avaient été diffusées dans un but incompatible avec leur finalité initiale.

En conséquence, l'autorité de contrôle a prononcé une amende de 3.000 € à l'encontre du propriétaire du bar.

Lien vers la décision en espagnol **:** https://bit.ly/3AI3HzR

Un centre d'imagerie médicale sanctionné pour avoir transféré les mauvaises données de santé

AEPD (ESPAGNE), 20 SEPTEMBRE 2021

Après avoir subi un accident du travail, un patient s'est rendu dans un centre d'imagerie médicale afin d'y réaliser une IRM. Le patient a, en parallèle, contacté sa compagnie d'assurance afin d'obtenir un congé maladie. La compagnie d'assurance a alors contacté le centre d'imagerie afin que ce dernier lui transmette le dossier médical du patient, et plus précisément le rapport de ladite IRM.

A cette occasion, le centre a fourni à l'assureur le rapport d'une précédente IRM du genou, que le patient avait réalisé à la suite d'une blessure contractée dans le cadre de ses activités domestiques.

L'assureur s'est référé à cet ancien rapport d'IRM pour estimer que l'accident s'était déroulé en dehors des heures du travail et ainsi refuser au patient le droit à un congé maladie.

Le patient a déposé une plainte auprès de l'autorité de contrôle qui a considéré que la divulgation du mauvais rapport d'IRM à la compagnie d'assurances constituait une violation du principe d'intégrité et de confidentialité (article 5(1)f du RGPD) et a ainsi infligé au centre d'imagerie une amende d'un montant de 18.000 €.

Lien vers la décision en espagnol : https://bit.ly/3j1NShe

Sanction d'une société d'exploitation autoroutière pour avoir transféré hors UE les données de millions d'automobilistes

DATATILSYNET (NORVEGE), 28 SEPTEMBRE 2021

L'autorité norvégienne de contrôle a ouvert une enquête à l'encontre de la FERDE, une société d'exploitation autoroutière, pour ses transferts de données personnelles à un sous-traitant en Chine entre septembre 2017 et octobre 2019.

Cette société, qui a pour mission d'enregistrer le passage des voitures pour lesquelles le télépéage ne fonctionne pas (ou des voitures non équipées d'un tel boitier), envoie plus de 12 millions d'images chaque année à son sous-traitant en Chine en charge de retravailler la qualité de l'image, lorsque nécessaire.

Au cours de son enquête, l'autorité de contrôle a d'abord relevé que la société avait un accord de traitement des données avec son sous-traitant, mais cet accord, non daté, n'était probablement pas en place au début des traitements.

L'autorité de contrôle a ensuite relevé que l'analyse d'impact effectuée pour ce type de traitement avait été antidatée et n'avait pas été mise en œuvre dès le début de la relation. L'autorité de contrôle a noté que, bien que l'article 32 du RGPD ne mentionne pas explicitement le moment auquel il convient de procéder à une évaluation des risques, il peut être déduit des articles 5(2), 24, 25 et 32 du RGPD qu'une telle évaluation doit avoir lieu avant le début des opérations de traitement en question.

Enfin, si la société avait signé les clauses contractuelles types de la Commission européenne pour le transfert de données personnelles vers des pays tiers, celles-ci n'étaient pas datées et ne semblaient pas avoir été mises en œuvre au début de la relation.

En conséquence, l'autorité de contrôle a infligé à la société une amende d'un montant de près de 5 000 000 € pour :

- (i) ne pas avoir conclu de contrat de sous-traitance encadrant le traitement des données personnelles (art 28(3)) ;

- (ii) ne pas avoir effectué d'analyse d'impact relative à la protection des données et de ce fait ne pas avoir respecté le principe d'intégrité et de confidentialité des données (article 5(1)f), ne pas être en mesure de démontrer que les principes relatifs au traitement des données à caractère personnel ont été respectés (article 5(2)) et ne pas avoir pu prendre les mesures techniques et organisationnelles nécessaires (article 32) ; et

- (iii) ne pas avoir mis en place de mécanisme de transfert de données personnes hors UE respectant les principes des articles 44 et suivants du RGPD.

Lien vers la décision en norvégien : https://bit.ly/3vdlUUw

Sanction du responsable d'un site pour y avoir inséré le patronyme et une photo de profil LinkedIn d'un individu

AEPD (Espagne) 13 septembre 2021

A la suite d'une plainte, l'autorité de contrôle espagnole a infligé une amende de 9.000 € au responsable d'un site internet qui avait publié l'identité du plaignant ainsi qu'une capture d'écran de son profil LinkedIn.

L'autorité de contrôle a considéré que le responsable du site n'avait pas obtenu le consentement de la personne concernée, en violation de l'article 6 du RGPD. De plus, le site ne possédant pas de politique de confidentialité, la personne était dans l'incapacité de connaître l'identité du responsable du site ou la façon dont il pouvait exercer ses droits, en violation de l'article 13 du RGPD.

Lien vers la décision en espagnol : https://bit.ly/3BKRFH2

VUE DANS LA PRESSE :

DROIT D'ACCES : DEMANDE GENERALE, REPONSE GENERALE

Face à une demande générale de droit d'accès, un organisme qui traite une grande quantité de donnée, devrait pouvoir se contenter d'une recherche générale sur les systèmes et fichiers les plus courants. Comme chaque mois, l'auteur tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions (publications) rendues par les autorités nationales de contrôle de protection des données personnelles au niveau européen ou par des juridictions étrangères.

Un citoyen hollandais a vu sa demande de droit d'accès rejetée par l'administration fiscale et douanière au motif qu'elle était si générale qu'elle s'apparentait à une « expédition de pêche ».

Le tribunal de district de Hollande du Nord n'a pas retenu cette position, considérant que l'administration aurait dû faire droit à cette demande en effectuant a minima une recherche « des plus courantes (. . .) dans les fichiers de données et/ou les systèmes/ applications informatiques les plus courants »[1]

RAPPEL DU PRINCIPE

En application de l'article 15 du RGPD, toute personne a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, obtenir l'accès auxdites données à caractère personnel ainsi, notamment, qu'aux informations suivantes : les finalités du traite-ment, les catégories de données à caractère personnel concernées, les destinataires auxquels les données à caractère personnel ont été ou seront communiquées et, lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée.

Par ailleurs, toute personne est en droit, sauf exceptions, d'obtenir du responsable du traitement une copie des données faisant l'objet du traitement. L'exercice du droit d'accès permet ainsi à toute personne de savoir si des données la concernant sont traitées et d'en obtenir la communication dans un format compréhensible.

Il permet également de contrôler l'exactitude des données afin, au besoin, de les faire rectifier ou effacer.

Le responsable du traitement, de son côté, est tenu de répondre à toute demande de droit d'accès. Les seuls cas dans lesquels il pourrait ne pas donner suite à une telle demande sont, comme le précise la Cnil[2], les suivants :

■ la demande est manifestement infondée ou excessive notamment par son caractère répétitif (par exemple : demandes multiples et rapprochées dans le temps d'une copie des données déjà fournie)

■ l'accès est impossible car les données ne sont plus conservées ou ont été effacées (par exemple : les enregistrements réalisés par un dispositif de vidéosurveillance qui sont détruits à l'issue d'un délai de 30 jours).

La circonstance selon laquelle la demande serait générique car portant sur l'ensemble des données traitées par un organisme ne permet pas, en revanche, à ce dernier de s'exonérer de son obligation. La Cnil indique d'ailleurs que, dans ce type de cas, et si la demande porte sur une grande quantité de données, le responsable du traitement peut inviter la personne concernée à préciser « sur quelles données ou quelles opérations de traitement porte sa demande (considérant 63 du RGPD) ».

2. LA POSITION DU TRIBUNAL DE DISTRICT DE HOLLANDE DU NORD

Dans cette affaire, l'administration fiscale et douanière avait rejeté une demande de droit d'accès d'un citoyen hollandais au motif qu'elle était trop générale.

Elle soutenait que la personne concernée aurait dû préciser sa demande, ce qu'elle n'a pas fait. En tout état de cause, pour l'administration, cette demande n'était pas légitime dès lors que la personne concernée pouvait accéder à une partie de ses données en consultant les onglets « Mes autorités fiscales » et « Mes abattements » du site internet de l'administration.

Selon le citoyen hollandais, il n'avait aucune obligation de préciser sa demande de droit d'accès et ce, d'autant plus qu'une demande spécifiée ne lui aurait pas permis un accès complet aux données traitées par l'administration, ce qui aurait laissé planer le risque que des données soient traitées de manière incorrecte et/ou incomplète et/ou illégale sans qu'il soit possible de vérifier et de corriger.

Le tribunal a, quant à lui, considéré que si un responsable du traitement peut demander des précisions s'il traite une grande quantité de données, « cela ne signifie pas qu'il peut dans tous les cas demander des éclaircissements avant d'effectuer une recherche ».

Selon le tribunal, « plus une demande est concrète, plus des efforts peuvent être attendus du responsable du traitement, mais (. . .) le responsable du traitement peut également être appelé à effectuer une recherche des données personnelles les plus courantes dans le cas d'une demande formulée de manière générale (…) dans les fichiers de données et/ou les systèmes/applications informatiques les plus courants ».

Considérant qu'en l'espèce l'administration fiscale et douanière ne démontrait pas, d'une part, qu'il était impossible d'effectuer une recherche des données personnelles les plus courantes dans un certain nombre d'applications ou de systèmes et, d'autre part, qu'une telle recherche ne nécessitait pas un « effort disproportionné », le tribunal de district de Hollande du Nord a jugé que la décision attaquée était insuffisamment motivée et l'a donc annulée.

3. QUELLES RECOMMANDATIONS ?

Face à une demande générale de droit d'accès, un organisme, qui traite une grande quantité de données, devrait pouvoir se contenter d'une recherche générale sur les systèmes et fichiers les plus courants, tout en précisant, dans sa réponse à la personne concernée, qu'il pourra affiner sa recherche à partir d'éventuels éclaircissements de la part de cette dernière.

Expertises, octobre 2021 – n°472
Un article rédigé par Maître Alexandre FIEVEE

(1) Tribunal de district de Hollande du Nord, 18 juin 2021, AWB- 20_ 4638.

(2) https://www.cnil.fr/fr/ professionnels-comment-repondre-une-demande-de-droit-d'accès

ACTUALITE DU CABINET

DERRIENNIC ASSOCIES PROPOSE UN PROGRAMME DE FORMATION DE **35 HEURES** POUR LA PRÉPARATION A LA CERTIFICATION DPO

OBJECTIF

1/ Acquérir les compétences, les connaissances et le savoir-faire attendus par la CNIL et permettre au collaborateur de se présenter à l'examen de certification en maximisant ses chances de succès.

2/ Indépendamment de la certification, la formation permet à l'apprenant de se familiariser avec la matière et d'acquérir les compétences, les connaissances et le savoir-faire pour :
analyser une situation impliquant un traitement de données personnelles ;
définir et appréhender les problématiques, les enjeux et les risques qui en découlent ;
prendre les décisions qui s'imposent en concertation avec l'équipe « DPO ».

CONTENU DE LA FORMATION

Partie 1 - Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité
Partie 2 - Responsabilité (Application du principe d'« Accountability »)
Partie 3 - Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

COUT

3000€ HT/personne

INTERVENANT

Alexandre FIEVEE
Avocat Associé
Tél : 01.47.03.14.94
afievee@derriennic.com

Classements
Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « Information Technology Law » (2020).
Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie « Next Generation Partners ».

RENSEIGNEMENTS PRATIQUES

Prochaine session 2021 :
Sur demande.
Lieu de la formation :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.
Inscription et informations :
afievee@derriennic.com