18 Bis Rue Molitor
75016 PARIS
contact@vertigo.energy
+33 (0)1 56 07 15 62

GUIDE RGPD PARTENAIRES

Juillet 2021

Ce guide a été conçu par le service de protection des données de Vertigo à destination des partenaires et sous-traitants de l'activité CEE. Il permet de rassembler des recommandations et bonnes pratiques quant à la mise en conformité des traitements des données dans le cadre du contrat de partenariat. Ainsi, cette aide dédiée n'est pas exhaustive et ne peut constituer le plan d'action de mise en conformité RGPD globale des partenaires.

Préambule et préalables

Qui est le Délégué à la Protection des données de Vertigo ?

Mme Florence OLIVE
Directrice Innovation & Marketing
florence@vertigo.energy
+33(0)6 44 16 56 10

Le RGPD encadre le traitement des données personnelles (DP) sur le territoire de l'Union Européenne. Tout organisme, peu importe sa taille, son pays d'implantation et son activité, doit s'y conformer.

Cette nouvelle règlementation constitue un enjeu important car en cas de manquement vous pouvez risquer jusqu'à :

4% de votre chiffre d'affaires pour chaque infraction ou jusqu'à 20 millions d'euros d'amende.

Qu'est-ce qu'une donnée personnelle ?

Toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne peut être identifiée : **directement** (nom, prénom) ou **indirectement** (identifiant, numéro de téléphone, avis d'imposition etc.)

L'identification d'une personne physique peut être réalisée à partir d'une seule donnée ou à partir du croisement d'un ensemble de données.

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles : il peut être informatisé mais les fichiers papiers sont également concernés.

Interdiction de collecter des données sensibles comme le numéro de sécurité sociale, de santé, religion etc. qui ne relèvent pas de notre finalité.

Un CSV d'opérations CEE, un carton de dossiers de valorisation de travaux de clients B2B ou B2C, une liste de SAV envoyé au bureau COFRAC est un traitement et doit être protégé !

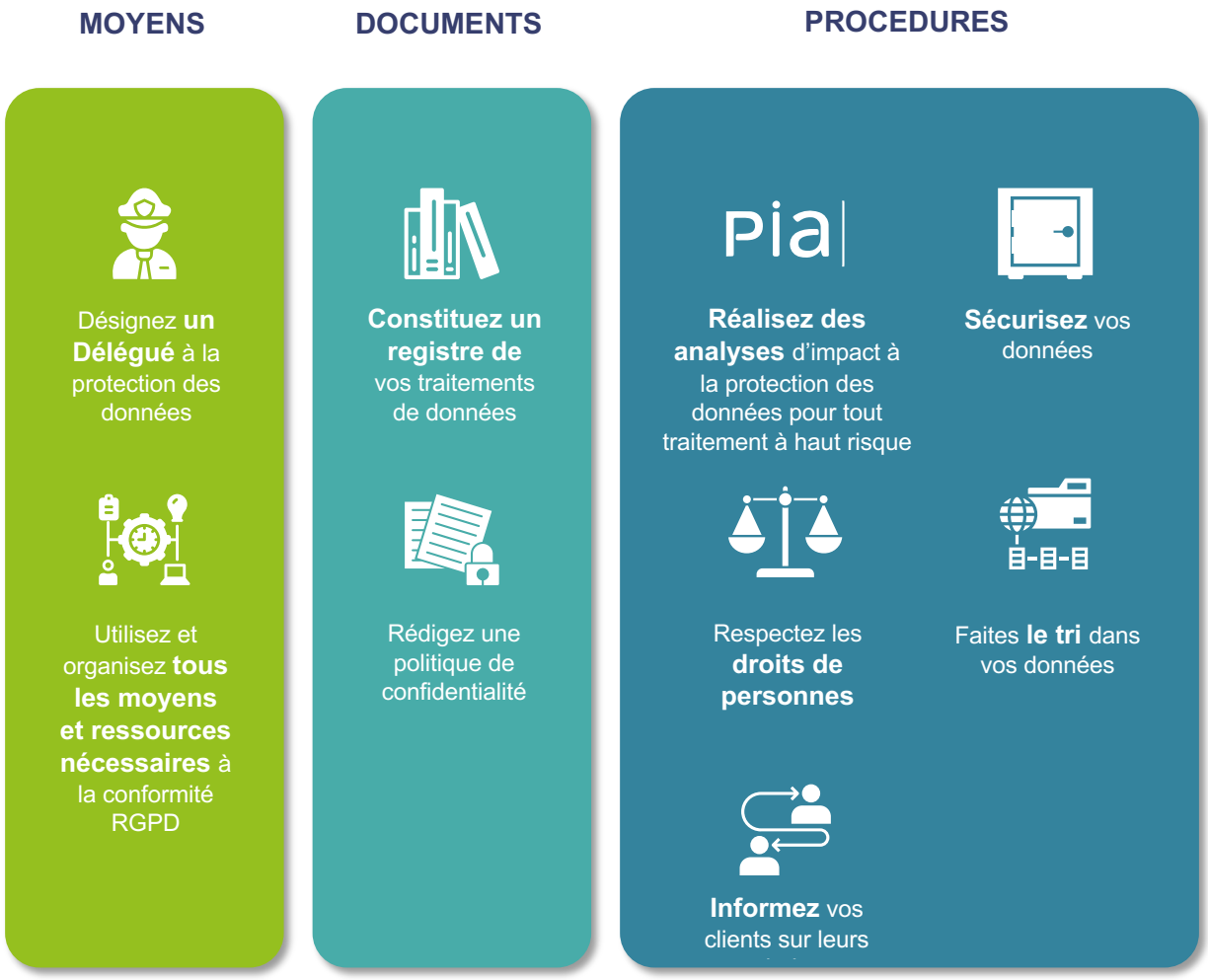
Cela s'applique donc au B2C mais aussi au B2B, car les adresses mails professionnelles (avec nom et prénom) ainsi que les numéros de téléphone pros constituent des DP.

Les 7 grands principes du RGPD

1. **Licéité, loyauté et transparence** : information du client sur les données collectées et leur utilisation, récupération du consentement obligatoire, etc.
2. **Limitation des finalités** : on utilise seulement les données pour les finalités déclarées et pour lesquelles le consentement est recueilli
3. **Minimisation des données** : récupérer le juste nécessaire pour réaliser la finalité
4. **Exactitude** : Obligation d'avoir des données tenues à jour, effacées ou rectifiées
5. **Limitation de la conservation** : Durée n'excédant pas celle nécessaire au regard des finalités, archives et utilisation de pseudonymes à des fins statistiques
6. **Sécurité des données** : Pouvoir assurer une protection des données physique, logistique et juridique
7. **Responsabilité** : être en conformité de façon continue et pouvoir le démontrer à chaque instant.

Les prérequis

La mise en conformité RGPD concerne tous les traitements de données effectuées dans l'entreprise (relevant de l'activité commerciale ou des données liées au fonctionnement interne). La réglementation vous oblige depuis mai 2018 à être en conformité et pouvoir le prouver à chaque moment en cas d'audit de la CNIL. Votre conformité au RGPD passera obligatoirement par l'établissement de documents, procédures et moyens que nous avons résumés de façon non exhaustive ci-dessous :



Quel est le rôle de Vertigo auprès des partenaires ?

En tant que responsable de traitement, Vertigo exige que tous ses partenaires mettent en place les moyens, mesures et ressources nécessaires au respect du RGPD. Au regard de l'interdépendance de nos traitements de données personnelles, Vertigo a intégré ses exigences minimales au contrat de partenariat, rendant **le partenariat conditionnel au bon respect et au suivi de la Réglementation en matière de Protection des Données.**

Et mes sous-traitants ?

Vous devez vous assurer que vos sous-traitants ont le **même niveau d'exigence** en matière de protection des données personnelles que vous. Il relève de votre responsabilité d'informer et suivre leur conformité et d'alerter le DPO de Vertigo en cas de manquement.

SOMMAIRE

A. INFORMER

1. COMMENT CONSTRUIRE UNE MENTION D'INFORMATION RGPD ?

Les mentions d'information RGPD sont obligatoires dès qu'il y a :

- **Collecte de données directe** (formulaire de contact, simulateur d'éligibilité dossiers CEE, email de contact en **B2C et B2B…)**
- **Transmission de données :** vous devez informer les clients de ce que vous faites de leurs DP (sous-traitance, collecte pour mandataire, etc.)
- **Collecte de données indirecte :** vous devez informer les clients sur l'origine (ex : achat de leads…)

Identité et coordonnées

Identité et coordonnées de l'organisme et du responsable de traitement

Finalités

A quoi vont servir les données collectées

Base légale

Base légale du traitement de données (ex : consentement des personnes, exécution d'un contrat, constitution du dossier CEE…)

Destinataires

Ou catégories de destinataires des données (qui a besoin d'y accéder ou de les recevoir au vu des finalités définies et consenties, y compris les sous-traitants)

Durée de conservation des données

Selon les termes du contrat avec Vertigo pour les dossiers CEE, 13 mois pour les cookies et traceurs

Droit des personnes concernées

Droits d'accès, effacement, rectification, portabilité, limitation, opposition, etc.

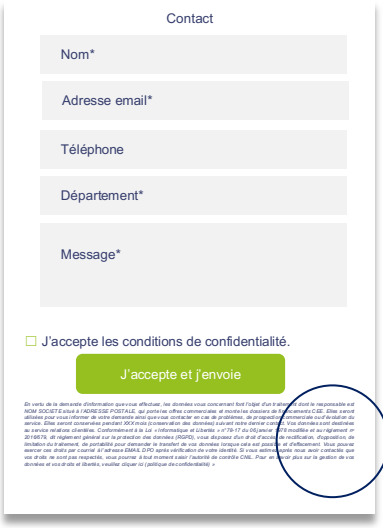
Coordonnées DPO

S'il a été désigné, ou alors ajouter les coordonnées du service compétent en la matière

Droit de réclamation auprès de la CNIL

Droit d'introduire une réclamation auprès de la CNIL par le client

Exemple mention d'information sous formulaire de contact :



« En vertu de la demande d'information que vous effectuez, les données vous concernant font l'objet d'un traitement dont le responsable est NOM SOCIETE situé à l'ADRESSE POSTALE, qui porte les offres commerciales et monte les dossiers de financements CEE. Elles seront utilisées pour vous informer de votre demande ainsi que vous contacter en cas de problèmes, de prospection commerciale ou d'évolution du service. Elles seront conservées pendant XXX mois (conservation des données) suivant notre dernier contact. Vos données sont destinées au service relations clientèles. Conformément à la Loi « Informatique et Libertés » n°78-17 du 06 janvier 1978 modifiée et au règlement nº 2016/679, dit règlement général sur la protection des données (RGPD), vous disposez d'un droit d'accès, de rectification, d'opposition, de limitation du traitement, de portabilité pour demander le transfert de vos données lorsque cela est possible et d'effacement. Vous pouvez exercer ces droits par courriel à l'adresse EMAIL DPO après vérification de votre identité. Si vous estimez après nous avoir contactés que vos droits ne sont pas respectés, vous pourrez à tout moment saisir l'autorité de contrôle CNIL. Pour en savoir plus sur la gestion de vos données et vos droits et libertés, veuillez cliquer ici (politique de confidentialité) »

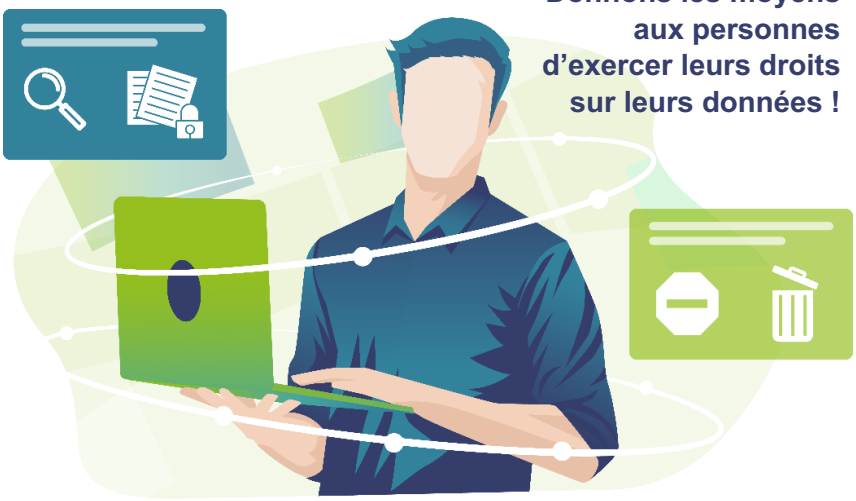
Pour l'exercice des droits des personnes concernées :
Différents droits peuvent être exercés : d'accès, d'effacement, d'opposition, portabilité, rectification et de limitation du traitement.

Bonne pratique : Soyez réactifs !

Bien traiter les demandes des consommateurs quant à leurs données personnels, c'est :

Renforcer la confiance qui sécurise la relation-client

Vous mettre à l'abri de critiques sur les réseaux sociaux, ou de réclamations auprès de la CNIL



Donnons les moyens aux personnes d'exercer leurs droits sur leurs données !

Mes clients sont vos clients ! Pensez à informer tout aussi rapidement vos sous-traitants et Vertigo en cas d'une demande client.

2. CONSENTEMENT

Concept central, le consentement doit être recueilli avant tout traitement de données et doit être répertorié dans un registre spécifique. La règlementation impose qu'il doit être donné de façon libre, spécifique, éclairée et univoque.

Le consentement en matière de prospection commerciale

B2C

Pas de prospection sans consentement explicite du destinataire au moment de la collecte de leur email.

Exceptions :

1. Si la personne prospectée est déjà cliente de l'entreprise et si ça concerne des produits ou services analogues à ceux déjà fournis
2. Si la prospection n'est pas de nature commerciale
   - Enregistrement du consentement dans un registre

B2B

Information et droit d'opposition. Les emails professionnels génétiques (contact@vertigo.energy) ne sont pas soumis aux principes du consentement et du droit d'opposition. L'objet de la sollicitation doit être en rapport avec la profession de la personne démarchée.

B2C et B2B

Au moment de la collecte de son adresse de messagerie, la personne doit :

- Être informée que son adresse électronique sera utilisée à des fins de prospection

Être en mesure de s'opposer à cette utilisation de manière simple et gratuite

Pour les formulaires de contact et de B2C

Recueillir le consentement préalable avec une case non-pré cochée et l'inscrire dans le registre des consentements.

Pour les datas brokers ou l'achat de leads

Informer la personne de la provenance de ses données

Vous pouvez programmer votre CRM pour qu'il enregistre le consentement à l'aide d'un horodatage lorsque quelqu'un accepte vos cookies ou lorsque la personne remplit un formulaire de contact

3. COLLECTE DES DONNEES

Les DP collectées doivent **être adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. A savoir la réalisation d'économie d'énergie pris en charge, tout ou partie, dans le cadre du financement via le dispositif CEE.

4. DUREE DE CONSERVATION MAXIMALE DES DONNEES

- **13 mois** maximum pour celles relatives aux **cookies et traceurs** liés à votre site internet et aux statistiques de mesures d'audiences (idem pour l'identité des visiteurs, données de connexion)
- **3 ans après le dernier contact** pour les données des **prospects** transmises par Vertigo qui n'ont pas pu aboutir à une valorisation des travaux. Pareil pour les **données clients** le temps de la relation commerciale.
- Indéfiniment pour les données anonymisées de manière irréversible ou pseudonymies à des fins archivistiques ou statistiques.

B. ACTIVITE CEE ET CAS PRATIQUES

1. ASTUCES ET BONNES PRATIQUES

Sur mon site internet

Intégrer une politique de confidentialité, des mentions légales et aussi mettre les mentions sous les formulaires de contact pour toute collecte de données personnelles

Les mentions suivantes constituent le minimum à avoir sur votre site web :

- Finalités traitement de DP
- Base juridique
- Caractère obligatoire ou non des réponses aux formulaires
- Destinataires des DP
- Nom du responsable de traitement
- Coordonnées DPO
- Mentions exercice des droits (accès, rectification, opposition etc.)
- Droit réclamation CNIL
- Transferts DP hors UE

- Gestion des cookies
- Bannière de consentement aux cookies
- Panneau de gestion des cookies

Les cases pré-cochées ne valent pas recueil du consentement

Sur une campagne d'appel

Rappeler la provenance des données personnelles utilisées (base, acceptation de réception des offres partenaires etc.)

Accompagner le recueil du consentement de la personne à l'oral par **l'envoi d'un mail de confirmation comportant les mentions RGPD qui rappelle leurs droits.**

Dans le temps d'attente et sur le message d'accueil, donner la possibilité d'accéder à la politique de confidentialité.

Enregistrer l'appel ne vaut pas recueil du consentement

Sur une campagne d'emailing

Rappeler la provenance des données personnelles utilisées : *« vous recevez cet email car vous vous êtes inscrits à XXX »*

Vous devez disposer du consentement des destinataires de la campagne

La personne doit avoir donné son consentement spécifique à une finalité déterminée. Exemple : Vous ne pouvez pas envoyer des campagnes à quelqu'un qui a uniquement consenti à recevoir un devis.

☐ *J'accepte de recevoir des informations sur les offres commerciales éligibles aux primes CEE XXX et ses partenaires*

Ajouter les mentions d'information RGPD

Proposer un moyen simple de s'opposer à la réception de nouvelles sollicitations comme avec un lien de désinscription en fin de mail

Pendant les salons événementiels

Vous devez demander le consentement de la personne concernée lors du moment de la collecte de ses données personnelles.

Vous pouvez imprimer des formulaires de consentement en format papier et les faire signer directement pendant le salon.

OU faites remplir un formulaire numérique avec des cases à cocher pour chaque finalité spécifique.

Remerciez votre visitorat en retour de salon par un mail comportant des mentions RGPD.

Conservez les preuves de recueil du consentement pour recevoir des offres sur le salon

Nouvelle campagne (privacy by design) – Réseaux sociaux

Minimiser les données personnelles collectées auprès des prospects.

Ajouter des mentions RGPD à chaque fin de mail et toujours renvoyer vers la politique de confidentialité.

Envoyez vos campagnes sur l'email dpo@vertigo.energy pour consultation et validation.

Demandez de l'aide et des conseils auprès du DPO dpo@vertigo.energy

2. DOCUMENTATION CEE

Les mentions d'information RGPD doivent être présentes lors de tout premier contact avec un client ou un prospect.

Soyez vigilants, c'est l'attestation sur l'Honneur (AH) qui comporte les mentions d'informations nécessaires à la valorisation des CEE. Elle comporte des mentions relatives au RGPD, aux traitements de données et à leur transmission aux mandataires et Obligés.

Ne ratez pas le **PREMIER CONTACT** avec vos clients ! Intégrez une ou plusieurs signatures d'email comportant les mentions d'informations adaptées

C. SECURITE

1. SECURITE

La sécurité des données personnelles relève aussi de votre responsabilité. Ci-dessous vous trouverez 7 catégories de bonnes pratiques pour établir votre **plan d'action** et assurer une sécurité optimale :

1- Sensibiliser et former

- Former et sensibiliser les collaborateurs aux enjeux de sécurité de base et des systèmes d'information

2- Connaitre le système d'information

- Identifier les infos et serveurs les plus sensibles et maintenir un schéma du réseau
- Organiser les procédures d'arrivée, départ et changement de fonctions utilisateurs

3- Authentifier et contrôler les accès

- Distinguer les rôles utilisateurs et administrateurs
- Imposer une politique de mot de passe robuste
- Privilégier une authentification forte si possible (Token, clé de chiffrement, clé PKI etc.)

4- Sécuriser les postes, le réseau et l'administration

- Sécuriser le parc informatique
- Chiffrer et sécuriser les données et transferts de données sensibles (Net Explorer etc.)
- Limiter au strict besoin opérationnel les droits administrateurs sur les postes de travail

5- Gérer le nomadisme

- Assurer une sécurisation physique des terminaux
- Avoir une charte informatique qui comprends le matériel nomade

6- Maintenir à jour le système d'information

- Définir une politique de gestion et mise à jour des logiciels

7- Superviser, auditer, agir

- Faire des sauvegardes régulières et instaurer la journalisation
- Procéder à des audits de sécurité réguliers et définir une procédure de gestion des incidents
- Définir un référent en sécurité des systèmes informatique et le faire connaitre du personnel

Points de vigilance en matière de sécurité

Le recours au **télétravail** suppose une vigilance accrue du fait de mauvaises pratiques qui favorisent des attaques par rançongiciels et hameçonnage à cause :

- De mauvaises configurations des outils de sécurité (VPN, mauvais paramétrages des contrôles d'accès etc.)
- D'un assouplissement non maîtrisé des mesures de sécurité (contournement de la restriction des adresses IP pour permettre le travail à distance etc.)
- De transmissions de données par email et divulgations non autorisées de données.

L'accès aux **locaux** doit être strictement encadré (badges, clés, sécurité ou alarme…)

Les coursiers devront signer un contrat avec votre société, pour assurer les courses et garantir la confidentialité des dossiers transportés (prévoir une indemnisation)

2. STOCKAGE - ARCHIVAGE ET DESTRUCTION DES DONNEES EN COURS ET FIN DE CONTRAT

Données personnelles collectées pour constituer et transmettre le(s) dossier(s) de financement via le dispositif CEE

Base active

Les données peuvent conservées dans la base active pour une durée couvrant toute la constitution du(des) dossier(s)

Peuvent rester dans la base active **6 mois** après la transmission des pièces du dossier à Vertigo en cas de contrôle ou demande d'information de Vertigo.

Archivage intermédiaire

Elles devront par la suite être archivées dans une base intermédiaire pendant une durée de 6 ans suite à la validation du montage des dossiers par Vertigo

Archivage définitif

Au terme de ces 6 années toutes les données devront être détruites ou intégrées à une base pseudonymisée.

Au terme du contrat et sans renouvellement

Détruire toutes les données à caractère personnel relatives au montage des dossiers CEE (copies comprises dans les drives systèmes d'information du sous-traitant).

Les données personnelles prospects

Les données transmises par Vertigo qui n'ont pu aboutir à une valorisation des travaux via le dispositif des CEE devront être détruites 3 ans après le dernier contact.

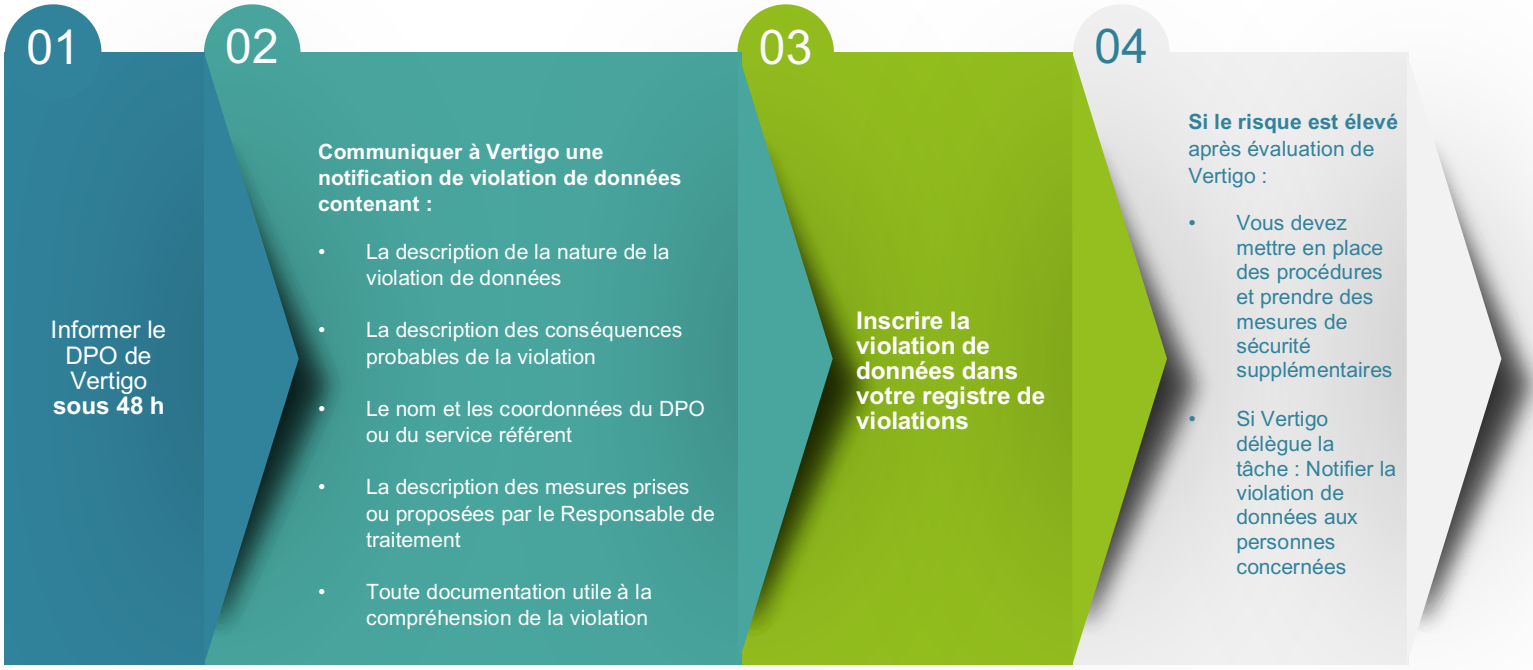
PV ou attestation de destruction

D. PROCEDURES

1. VIOLATION DES DONNEES

Une violation de données à caractère personnel (DCP) est une **violation de la sécurité** entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non-autorisée de DCP transmises, ou bien l'accès non autorisé à ces données. D'origine malveillante ou non, ce qui peut entrainer comme conséquence de compromettre leur intégrité, confidentialité ou disponibilité.

En cas de violation de données :



Il peut s'agir de la perte d'un dossier ou d'un document par un transporteur ; du vol d'un ordinateur portable ou d'un téléphone professionnel ; de l'attaque du site web de votre société ou par rançongiciel etc.

2. AUDITS RGPD

Vertigo peut aussi réaliser des **audits RGPD** auprès de ses partenaires, nous le faisons déjà sur vos sites web de façon récurrente. Il est également possible que vous fassiez l'objet d'un Audit RGPD interne, pour lequel nous irons directement vous **auditer sur site** et nous pouvons être amené à vous demander des documents comme vos registres de traitements, AIPD, registre des consentements, politique de confidentialité etc.

En cas de nombreux manquements au RGPD ou violations de données, nous pourrons vous auditer sur site.

3. EXEMPLE DE PV OU ATTESTATION DE DESTRUCTION DES DONNEES

Attestation de destruction des données personnelles collectées dans le cadre du Contrat de partenariat/mandat avec Vertigo

Je soussigné(e),

Monsieur/Madame ……., gérant/délégué à la protection des données/responsable de traitement de la société ……,

Domiciliée à l'adresse suivante :

……..
……..

N°SIRET : ……

Atteste avoir procédé ou fait procéder à la destruction :

- Des données à caractère personnel relatives au montage des dossiers CEE (copies comprises dans les divers systèmes d'information du sous-traitant) au terme de mon contrat et sans renouvellement de celui-ci.
- Des données personnelles prospects transmis par Vertigo qui n'ont pu aboutir à une valorisation des travaux via le dispositif des CEE devront être **détruites 3 ans après le dernier contact**.
- Des données personnelles collectées pour constituer et transmettre le(s) dossier(s) de financement via le dispositif CEE **après les 6 ans d'archives dans une base intermédiaire pendant une durée de 6 ans** suite à la validation du montage des dossiers par Vertigo

Cette destruction a été effectuée dans des conditions à garantir le respect de la confidentialité des informations contenues dans les dossiers et fichiers, sous peine des sanctions pénales prévues aux articles 226-21 et 226-22 du code pénal.

Fait le ……/……../…….. à
……

Signature et tampon

NB : En cas de recours à un prestataire, joindre le procès-verbal de destruction fourni par celui-ci.