

POLITIQUE DE PROTECTION DES DONNEES À CARACTERE PERSONNEL¹

La protection de vos données au sein de la CNETP

- **RGPD, quels impacts pour vous ?**

Le RGPD² vise à vous donner **plus de contrôle, de sécurité et d'accès** à vos données à caractère personnel, c'est donc une amélioration dans la **transparence** de l'utilisation de vos données.

RAPPEL ! Une donnée à caractère personnel correspond à toute information se rapportant à une personne physique, identifiée ou identifiable. Notamment son nom, son prénom, son NIR, son adresse email, etc.

- **Quel est notre engagement ?**

La CNETP s'engage à **respecter l'ensemble de vos droits et de ses obligations** en engageant des actions concrètes.

A cet effet, un **comité de pilotage mensuel** (auquel participe le DG, le SG, le DSI, le DPO et le responsable réseau) se consacre à la mise en conformité du règlement et est en charge de son maintien. Un **Délégué à la protection des données (DPO)** a été désigné pour en être pilote.

Qui est notre DPO ?

DPO est l'acronyme de Data Protection Officer, c'est-à-dire Délégué à la Protection des Données.

Nom du DPO : Karine GANDON

Le délégué est joignable : dpo@cnetp.fr

Quel est son rôle ?

- **Chef d'orchestre**

Il est le « *chef d'orchestre* » de la conformité en matière de protection des données à caractère personnel au sein de la CNETP (responsable de traitement). Pour rappel, il **n'est pas responsable juridiquement** des possibles violations du RGPD.

- **Point de contact**

Il fait office de point de contact avec nos clients, nos fournisseurs, nos collaborateurs, notre direction, l'autorité de contrôle et toute autre partie prenante de l'organisme

- **Information/sensibilisation**

Il est chargé de sensibiliser, d'informer et de conseiller l'ensemble du personnel de la CNETP sur la protection des données à caractère personnel et ainsi de développer une culture interne en la matière.

¹ Document établi en décembre 2021.

² Règlement général sur la protection des données du 27 avril 2016 entré en vigueur à compter du 25 mai 2018

- **Contrôles**

Il est chargé de contrôler la réglementation RGPD au sein de la CNETP et veiller au respect de l'ensemble des procédures. Il assurera notamment les audits internes des services et les audits de contrôle chez les sous-traitants.

Engagement en tant que Responsable de Traitement

En tant qu'entreprise de Travaux Publics légalement tenue de s'affilier à la CNETP conformément aux dispositions légales, la Caisse traite les données personnelles que vous lui confiez en tant que responsable de traitement.

Le responsable de traitement est donc la CNETP, incarnée par son représentant légal.

Pour ce faire, la CNETP respecte **5 grands principes** issus du RGPD :

- ❖ **Principe de finalité**

La CNETP ne peut collecter et utiliser des données personnelles que dans un but défini et légitime

- ❖ **Principe de proportionnalité**

Les données collectées doivent être pertinentes et strictement nécessaires pour atteindre la finalité définie

- ❖ **Principe de limitation de la conservation**

Les données ne peuvent pas être conservées éternellement : une durée de conservation doit être fixée pour chaque donnée selon sa finalité

- ❖ **Principe de sécurité et confidentialité**

La CNETP doit garantir la sécurité et la confidentialité des données détenues. Chaque collaborateur doit donc respecter les directives internes concernant la sécurité numérique et ne doit jamais divulguer les données auxquelles il peut avoir accès.

- ❖ **Droits des personnes**

La CNETP doit garantir et faciliter la mise en œuvre des droits des personnes physiques pour qu'elles gardent la maîtrise de leurs données (*accès, rectification, effacement, etc.*)

Engagement vis-à-vis de nos Sous-Traitants

RAPPEL ! Un sous-traitant, selon le RGPD, est celui qui traite des données personnelles pour le compte d'un responsable de traitement (ex : fournisseur informatique, etc.).

Interroger l'ensemble de nos sous-traitants et leur faire signer un avenant au contrat initial afin d'être conforme aux exigences issues du RGPD

Contrôler leurs code de conduite, leurs politiques à l'égard des données personnelles, les coordonnées de leurs DPO ou équivalent, et toutes autres preuves nous permettant d'assurer les engagements de sécurité liés au RGPD, notamment leurs registres des traitements clients et leurs procédures d'alerte

Mener des audits réguliers

L'humain : notre force

Nos collaborateurs sont tous soumis à un engagement de confidentialité.

Ils sont sensibilisés et formés dès leur embauche au cours d'un entretien spécifique consacré au RGPD, et ceux déjà en poste ont tous suivi une formation de sensibilisation.

Par la suite plusieurs campagnes sont menées :

- des rappels diffusés par mail,
- des quizz organisés pour s'assurer du bon maintien des connaissances,
- des audits annuels des services,
- l'ensemble des supports de sensibilisation/d'information rassemblé dans une rubrique dédiée "DPO" sur l'intranet de la CNETP, auxquels sont ajoutés des fiches thématiques et des questions/réponses

L'engagement de la Direction

La CNETP travaille à partir de données nominatives sensibles et c'est pourquoi, il convient d'être particulièrement vigilant quant à leur intégrité. C'est tout le sens de la démarche engagée par la CNETP pour la mise en œuvre du RGPD, qu'il s'agisse de la désignation d'un DPO en la personne de Karine GANDON, du suivi régulier des actions RGPD par le comité de pilotage mensuel, ou bien encore de la mise en place d'un SOC (*centre opérationnel de sécurité*). C'est également notre engagement à l'égard des employeurs de la Profession et de leurs salariés.

LE DIRECTEUR GENERAL



L. BENEZIT

Des actions concrètes pour une mise en conformité

Elargissement des droits des personnes concernées par le traitement des données personnelles

- consentement éclairé
- **mentions d'information**
- gestion des droits
- **procédure d'alerte en 72 h**

Responsabilité accrue du sous-traitant en matière de protection des données

- annexe contractuelle conformité au RGPD
- audit de contrôle

Sensibilisations et formations

- charte informatique annexée au règlement intérieur
- engagement de confidentialité
- quizz/OCM réguliers
- intranet rubrique dédiée "DPO/protection des données"

Documentations

- charte informatique annexée au RI
- **registre des traitements mis en œuvre**
- cartographie des données
- PCA

Renforcement des contrôles internes des process de protection des données

- comité pilotage RGPD
- feuille de route des actions de mise en conformité et suivi
- audit interne et audit par CIBTP France (*tête de réseau des Caisses de congés*)
- audit interne des services
- intranet rubrique dédiée protection DCP

DSI

- **élaboration d'un schéma directeur à 3 ans**
- privilège donné au cloud souverain (*prestataires français avec infrastructures situées en France*)
- toutes mesures de sécurité adéquates (*pare-feu, protection des cyberattaques véhiculées par emails*)
- renforcement des compétences sécurité SI

Contrôles permanents

- analyse des risques
- **études d'impact réalisées sur les missions "cœur de métier"** de la CNETP

Sécurisation des traitements

- **utilisation d'outils informatiques sécurisés**
- nouveau site de back up
- **mise en place d'un SOC** (*Centre opérationnel de sécurité*)
- cryptage mots passe pour accès espaces sécurisés