



## **INSTRUCTIONS GÉNÉRALES À L'INTENTION DES RESPONSABLES ET DE SUJETS CHARGÉS DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL**

Voici les instructions à suivre lorsque vous effectuez des opérations de traitement des données personnelles dans le cadre de votre domaine. Nous vous rappelons que toute information se rapportant à une personne physique identifiée ou identifiable constitue une " donnée à caractère personnel". De même, toute opération ou ensemble d'opérations, réalisées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou à des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation , l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, la comparaison ou l'interconnexion, la limitation, l'effacement ou la destruction, constitue une opération de "traitement" et, en tant que telle, doit être effectuée dans le respect de ces instructions.

En confirmant que les lignes directrices opérationnelles fournies jusqu'à présent sont conformes aux buts et méthodes mentionnés dans le MSG « Vie Privée et protection de données », nous déclarons par la présente les règles de conduite qui doivent être observées lors du traitement des données personnelles :

- n'acquérir que les données personnelles nécessaires et suffisantes pour atteindre les objectifs dont votre unité de travail est chargée ;
- fonctionner conformément aux présentes instructions et à toutes les instructions spécifiques qui peuvent être données concernant des activités/traitements spécifiques ;
- collecter et enregistrer des données personnelles exclusivement pour l'inclusion dans les bases de données à disposition de l'unité, conformément au système normatif en vigueur, et pour les traiter afin de poursuivre les objectifs commerciaux assignés à l'unité ;
- dans le cadre de vos pouvoirs, veiller à l'exactitude et à la mise à jour en temps utile des données;
- veiller avec la diligence requise à ce qu'aucune donnée personnelle non pertinente, inutile ou superflue ne soit conservée dans l'unité, conformément aux principes énoncés dans le MSG « Vie Privée et protection de données » et dans la section spécifique "privacy" de l'intranet ;

- veiller, conformément aux règles de prudence et de diligence, à traiter les données personnelles avec la plus grande confidentialité et à empêcher aux tiers non autorisés de prendre connaissance des données détenues, notamment en adoptant des mesures de sécurité appropriées à l'égard du traitement des données à caractère personnel.;
- n'effectuer que les opérations de traitement auxquelles vous êtes autorisé, en suivant les instructions reçues ;
- en cas de retrait, même temporaire, du poste de travail, vérifier qu'il n'existe aucune possibilité pour les personnes extérieures à l'unité (même si elles appartiennent à la fonction) d'accéder aux données à caractère personnel faisant l'objet d'un traitement, sur support papier ou par voie électronique..

Il est absolument interdit de communiquer à quiconque le mot-clé nécessaire pour accéder aux bases de données contenant des données personnelles.

Les obligations de confidentialité, de communication et de diffusion doivent être scrupuleusement respectées par vous, même après la cessation de la relation de travail en cours avec l'entreprise.

En ce qui concerne les mesures de sécurité dans le traitement des données, nous vous donnons, ci-dessous, les directives opérationnelles à respecter avec soin, afin d'éviter le risque d'accès non autorisé au système informatique et la perte et / ou la destruction, même accidentelle, de données personnelles ou le traitement non autorisé de celles-ci :

- 1) en ce qui concerne les archives papier, contrôler et conserver, pendant toute la durée des opérations de traitement, les actes et documents contenant des données à caractère personnel afin d'empêcher qu'ils ne soient consultés et rendus accessibles par des personnes non autorisées. Dans le cas de documents contenant des catégories particulières de données à caractère personnel, les conserver dans des fichiers verrouillables et en limiter l'accès, en l'accordant exclusivement aux personnes autorisées et/ou responsables désignés par le responsable du traitement ;
- 2) pour accéder aux données sous forme électronique, utiliser des mots de passe et autres identifiants d'authentification attribués par le Responsable et/ou le Sous-traitant et/ou l'administrateur du système désigné par le Responsable ;
- 3) préserver la confidentialité des mots de passe et protéger avec diligence les dispositifs d'accès aux systèmes d'information, en votre possession exclusive ;
- 4) se conformer à toute procédure de gestion des identifiants d'authentification adoptées par le Responsable et/ou le Sous-traitant et/ou l'administrateur du système ;
- 5) si des supports informatiques amovibles (par exemple des dispositifs portables) sont utilisés pour stocker des données à caractère personnel, ils doivent être conservés de manière à prévenir la destruction, la perte, l'accès non autorisé et le traitement non autorisé des mêmes données. En particulier, pendant leur utilisation, ces supports doivent être conservés dans des armoires verrouillables, accessibles exclusivement au personnel mandaté à cet effet et objet d'un accès surveillé et

enregistré (après l'heure de fermeture). Ils ne devraient également être accessibles qu'à la suite de l'interaction avec les systèmes d'authentification et de cryptage ;

6) formater des supports informatiques amovibles contenant des données à caractère personnel une fois que les motifs de conservation ne s'appliquent plus ;

7) se conformer aux dispositions de tout plan de sécurité adopté par le Responsable et/ou le Sous-traitant et/ou l'administrateur du système en tenant compte des procédures appliquées par l'entreprise.

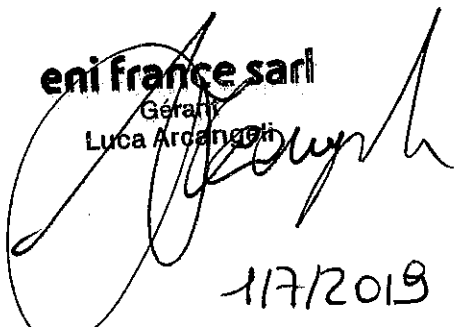
Vous devez également observer les règles de conduite suivantes :

- informer le Sous-traitant du traitement de référence sur les demandes des parties intéressées et l'aider dans la gestion correcte de celles-ci, en conformité avec le MSG Vie Privée et protection de données ;
- si vous avez connaissance d'une violation potentielle qui entraîne ou peut entraîner la destruction, la perte, la modification, la divulgation non autorisée ou l'accès aux données personnelles, informer rapidement le Sous-traitant du traitement des données et coopérer avec le même sujet dans la gestion de la violation, comme prévu dans le MSG Vie Privée et protection de données ;
- aider le Sous-traitant du traitement des données de référence dans l'établissement des registres pour les activités de traitement et dans la compilation des rapports périodiques.

Ces instructions sont valables pour toute la durée de la relation contractuelle / contrat de travail entre les parties, à l'exception du droit de les mettre à jour, de les révoquer ou de les compléter à tout moment, de la part du Délégué du Responsable du traitement.

En cas de cessation du contrat de travail, vous devez interrompre toutes les opérations de traitement des données et, dans la mesure du possible, restituer immédiatement les données ou les détruire, sous réserve d'autorisation du Sous-traitant du traitement.

Délégué du Responsable du traitement des Données Personnelles

**eni france sarl**  
Gérant  
Luca Arcangeli  
  
11/7/2019