MEOGROUP

POLITIQUE DE PROTECTION DES DONNÉES PERSONNELLES

DIRECTION DES SYSTÈMES D'INFORMATION & DES TECHNOLOGIES
03/04/2025

SOMMAIRE

GESTION DES VERSIONS

VERSION	AUTEUR	RÔLE	DATE
1.0	Anaïs LANGEVIN *Corporate Chief Information Officer* *Corporate Data Protection Officer*	Rédacteur	03/04/2025
	Frédéric DUPONT *Chargé de communication et marketing EIPM* *Data Protection Officer EIPM*	Relecteur	14/04/2025
	Alice GASNIER *Corporate Chief Compliance Officer*	Relecteur	22/04/2025
	Lisa PUDDU *Quality engineer*	Relecteur	22/04/2025
	Bilal AIT-GACEM *Corporate IT & Security Project Leader*	Relecteur	11/04/2025
	Célia YVAIN *Corporate Chief HR Officer*	Relecteur	14/04/2025

GLOSSAIRE

- **Autorité de contrôle :**
  Organisme national chargé de veiller à l'application de la réglementation en matière de protection des données personnelles.

- **Base légale :**
  Justification juridique permettant de traiter des données personnelles en conformité avec la règlementation locale.

- **Données personnelles (DP) :**
  Toute information se rapportant à une personne physique identifiée ou identifiable (ex. : nom, prénom, adresse e-mail, numéro de téléphone, adresse IP).

- **Données personnelles sensibles (DPS) :**
  Catégorie particulière de données personnelles incluant, par exemple, les informations relatives à la santé, aux origines raciales ou ethniques, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, ou encore aux données biométriques et génétiques.

- **Espace Économique Européen (EEE) :**
  Zone comprenant les États membres de l'Union européenne ainsi que l'Islande, le Liechtenstein et la Norvège.

- **Personne concernée :**
  Individu dont les données personnelles sont collectées et traitées.

- **Responsable de traitement (RT) :**
  Entité (personne physique ou morale) qui détermine les finalités et les moyens du traitement des données personnelles.

- **Sous-traitant (ST) :**
  Entité qui traite des données personnelles pour le compte et sur instruction d'un responsable de traitement.

- **Traitement de données personnelles :**
  Toute opération effectuée sur des données personnelles, qu'elle soit automatisée ou non.

- **Violation de données personnelles :**
  Atteinte à la sécurité des données entraînant leur destruction, leur perte, leur altération, leur divulgation non autorisée ou leur accès non autorisé.

INTRODUCTION

Fondé en 2005 par Richard Caron, MEOGROUP est un groupe de conseil en performance des entreprises, opérant en France et à l'international. Fort de plus de 850 collaborateurs, le groupe génère un chiffre d'affaires de plus de 100 millions d'euros.

MEOGROUP se compose de 10 cabinets spécialisés en conseil et prestation, management de transition et recrutement, ainsi que d'un institut de formation. Nos domaines d'expertise incluent les Achats & Supply Chain, la Finance & Contrôle de Gestion, et la Gestion de Projets & Transformation (Industriel, IT, Architecture & Design).

Les consultants de MEOGROUP accompagnent des entreprises de tous secteurs, des grands comptes aux startups, dans leurs projets de transformation et d'amélioration de la performance.

ENGAGEMENT EN FAVEUR DE LA PROTECTION DES DONNÉES PERSONNELLES

MEOGROUP accorde une importance capitale à la sécurité et à la confidentialité des données personnelles qu'il collecte et traite.

En conformité avec les exigences légales, le groupe met en œuvre des mesures strictes pour garantir la protection de ces informations et assurer leur traitement dans le respect des droits des individus.

MEOGROUP s'engage à ne collecter que les données nécessaires, à les conserver de manière sécurisée et à les traiter de façon transparente et responsable. La confiance de ses clients, partenaires et collaborateurs est essentielle, et le groupe déploie tous les moyens nécessaires pour protéger leurs données contre toute utilisation abusive, accès non autorisé, altération ou divulgation non autorisée.

OBJECTIF DE CE DOCUMENT

L'objectif principal de cette politique de protection des données personnelles (PPDP) est d'assurer la sécurité, la confidentialité et la conformité des données personnelles collectées, traitées et conservées par le groupe.

Cette politique vise à respecter les droits des individus en garantissant une gestion transparente et responsable de leurs informations personnelles. Elle se conforme aux exigences légales et met en place des mesures de sécurité rigoureuses pour protéger les données contre tout accès non autorisé, toute altération ou toute perte.

En instaurant des pratiques sécurisées et en sensibilisant l'ensemble des parties prenantes, MEOGROUP s'engage à protéger la vie privée des individus tout en minimisant les risques juridiques et opérationnels pour l'entreprise.

RÉVISION DE CE DOCUMENT

Le présent document fait l'objet d'une révision périodique afin de garantir son adéquation avec les exigences légales, réglementaires et organisationnelles en vigueur. Cette révision intervient au minimum une fois tous les trois ans ou à la suite de tout changement significatif pouvant impacter la gestion des données personnelles.

Toute mise à jour est réalisée sous la supervision du Corporate Data Protection Officer (DPO) en concertation avec les parties prenantes concernées. Les modifications apportées sont communiquées aux personnes concernées.

PÉRIMÈTRE D'APPLICATION

PERSONNES CONCERNÉES

Sauf mention contraire, la présente politique s'applique à l'ensemble des interlocuteurs de MEOGROUP.

MARQUES CONCERNÉES

Sauf mention contraire, la présente politique s'applique à l'ensemble des marques qui composent MEOGROUP :

- Adven,
- Axel,
- Cadele,
- Cost House,
- Cristal Décisions,
- EIPM,
- Luca,
- Masai,
- Meotec,
- SolvHA,
- Sowing,
- Valoptia.

PAYS CONCERNÉS

Sauf mention contraire, la présente politique s'applique à l'ensemble des pays dans lesquels MEOGROUP agit :

- La Belgique,
- Le Brésil,
- Le Canada,
- L'Espagne,
- La France,
- L'Italie,
- Le Luxembourg,
- Le Maroc,
- La Suisse.

CONTEXTE LÉGISLATIF

Dans le cadre de la protection des données personnelles, MEOGROUP se conforme aux exigences légales et réglementaires en vigueur, en particulier celles prévues par le Règlement Général sur la Protection des Données (RGPD) et les autres législations applicables au niveau national et international.

- **Belgique** :
  - Règlement Général sur la Protection des Données (RGPD),
  - Loi relative à la protection des données personnelles qui complète et transpose le RGPD en Belgique et est régulée par la Commission de la protection de la vie privée (Autorité de protection des données, APD).

- **Canada** :
  - Loi fédérale sur la protection des renseignements personnels et les documents électroniques (LPRPDE) qui régit la collecte, l'utilisation et la divulgation des renseignements personnels dans le secteur privé,
  - Loi sur la protection des renseignements personnels dans le secteur privé (Loi 25).

- **Espagne** :
  - Règlement Général sur la Protection des Données (RGPD),
  - Loi organique 3/2018 sur la protection des données personnelles et la garantie des droits numériques, qui complète le RGPD en tenant compte des spécificités nationales et des droits numériques. Elle est supervisée par l'Agence espagnole de protection des données (AEPD).

- **France :**
  - Règlement Général sur la Protection des Données (RGPD),
  - Loi Informatique et Libertés, qui complète le RGPD et précise des aspects spécifiques de la protection des données. Elle est supervisée par la Commission Nationale de l'Informatique et des Libertés (CNIL).

- **Italie :**
  - Règlement Général sur la Protection des Données (RGPD),
  - Code de la vie privée, qui est régie par le Code de la vie privée (Décret législatif n° 196/2003), mis à jour pour se conformer au RGPD. Elle est régulée par le Garant pour la protection des données personnelles.

- **Luxembourg :**
  - Règlement Général sur la Protection des Données (RGPD),

- Loi du 1er août 2018 relative à la protection des données personnelles, qui complète le RGPD en clarifiant certains aspects spécifiques à Luxembourg et est supervisée par la Commission nationale pour la protection des données (CNPD).

> **Maroc :**

- Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, qui encadre le traitement des données personnelles. Elle est supervisée par la Commission Nationale de contrôle de la protection des données à caractère personnel (CNDP).

> **Suisse :**

- Loi fédérale sur la protection des données (LPD),
- Règlement sur la protection des données (RPD), qui accompagne la LPD et précise les modalités de mise en œuvre des règles de protection des données.

ORGANISATION AUTOUR DE LA PROTECTION DES DONNÉES PERSONNELLES

L'organisation de la protection des données personnelles consiste à définir les équipes en charge de la sécurité, les responsabilités et la gouvernance.

LA DÉLÉGUÉE À LA PROTECTION DES DONNÉES (DPO)

La DPO définit et pilote la politique de protection des données personnelles de MEOGROUP.

Notamment, elle est amenée à :

- Veiller à la conformité avec les réglementations applicables,
- Superviser la documentation,
- S'assurer du respect des droits des personnes,
- Arbitrer les risques avec la Direction
- Conseiller les équipes projet et accompagne la mise en œuvre des recommandations,
- Participer aux audits, notifier les violations aux autorités compétentes, coopérer avec les autorités de contrôle,
- Sensibiliser les collaborateurs.

LA DIRECTRICE DES SYSTÈMES D'INFORMATION (DSI)

La DSI définit la stratégie IT du groupe et garantit la sécurité, la disponibilité et l'intégrité des données.

Notamment, elle est amenée à :

- Piloter les projets informatiques,
- Gérer les risques liés aux systèmes d'information,
- Déployer les mesures de protection des données personnelles (chiffrement, traçabilité, sauvegardes, etc.).
- Gérer des incidents de sécurité impliquant des données personnelles, en apportant une réponse technique adaptée et documentée,
- Intégrer les exigences de protection des données dans tous les projets SI.

LA DIRECTRICE DES RESSOURCES HUMAINES (DRH)

La DRH définit les politiques RH en lien avec la stratégie du groupe.

Notamment, elle est amenée à :

- S'assurer que les traitements de données relatifs aux salariés, candidats et collaborateurs respectent les obligations en vigueur.
- Participer aux analyses d'impact, mettre en œuvre des mesures de confidentialité adaptées,
- Travailler avec le DPO et la DSI pour sécuriser les projets RH (recrutement, paie, formation, etc.).

LA DIRECTRICE DE LA CONFORMITÉ (DC)

La DC coordonne le dispositif global de conformité réglementaire et éthique de MEOGROUP.

Notamment, elle est amenée à :

- Élaborer les politiques internes,
- Organiser les contrôles et audits,
- Superviser les formations en lien avec les obligations légales (anticorruption, données personnelles, éthique, etc.).

LE RESPONSABLE DE LA SÉCURITÉ INFORMATIQUE (RSSI)

Le RSSI pilote la sécurité du système d'information de MEOGROUP.

Notamment, il est amené à :

- Définir les règles de sécurité,
- Sensibiliser les collaborateurs,
- Superviser les plans de reprise d'activité,
- Assurer le suivi des incidents de sécurité.

NOTRE GOUVERNANCE CROISÉE

Processus / Activité	DPO	DSI	DRH	DC	RSSI
Définition de la politique	P	C	C	PC	C
Mise en conformité / audits	P	C	C	PC	C
Privacy by Design / Privacy by Default	P	PC	C	C	PC
Réalisation d'analyses d'impacts	P	C	C	C	C
Gestion des incidents de sécurité	C	PC	C	C	P
Notification aux autorités de contrôle / information aux personnes concernées	P	C	S	C	S
Traitement des droits des personnes	P	S	PC	C	S
Gestion du registre des traitements	P	F	F	S	F
Sensibilisation des collaborateurs	P	S	PC	PC	PC
Veille réglementaire et conformité internationale	P	S	S	CP	S

P = pilote ; C = contributeur ; S = support ; CP = co-pilote ; F = fournisseur d'information

GESTION DES DONNÉES PERSONNELLES

OUTIL DE SUIVI DE LA CONFORMITÉ

MEOGROUP s'appuie sur la solution Data Legal Drive, de l'éditeur EQS Group pour piloter au quotidien la conformité, notamment à travers la tenue du registre des traitements et la gestion des demandes des personnes concernées.

TRAITEMENT DES DONNÉES PERSONNELLES

MEOGROUP traite des données personnelles dans le cadre de ses activités de conseil, en conformité avec les réglementations applicables. Ces traitements concernent principalement la gestion des salariés, la relation avec les candidats, les clients et les partenaires, ainsi que l'amélioration des services proposés.

Les données collectées sont traitées de manière licite, loyale et transparente, et sont limitées aux finalités déterminées et légitimes. Elles sont conservées pour une durée strictement nécessaire à la réalisation de ces finalités, conformément aux obligations légales et aux recommandations des autorités de protection des données. À l'issue de cette durée, elles sont supprimées, anonymisées ou archivées de manière sécurisée. Elles font l'objet de mesures de sécurité appropriées afin d'en garantir la confidentialité, l'intégrité et la disponibilité.

Une description détaillée des traitements effectués, incluant les bases légales, les catégories de données et les durées de conservation, est consignée dans le registre des traitements tenu à jour, sous la supervision du DPO.

APPLICATION DES PRIVACY BY DESIGN ET PRIVACY BY DEFAULT

MEOGROUP applique les principes de Privacy by Design et Privacy by Default à chaque projet impliquant des données personnelles. Cela signifie :

- Anticiper les risques dès la conception,
- Ne collecter que les données strictement nécessaires,
- Mettre en place par défaut des paramètres de confidentialité élevés,
- Réserver l'accès aux seules personnes autorisées,
- Sensibiliser les équipes projet et métier à ces exigences.

Ces principes sont intégrés dans les outils, les processus, et la formation des collaborateurs.

ANALYSE D'IMPACTS (AIPD / DPIA)

Une Analyse d'Impact sur la Protection des Données est réalisée lorsqu'un traitement de MEOGROUP présente un risque élevé pour les droits et libertés des personnes. Elle permet d'identifier les risques et de proposer des mesures correctives adaptées.

Lorsque cela est nécessaire, MEOGROUP consulte l'autorité de contrôle compétente avant la mise en œuvre du traitement concerné.

Les collaborateurs impliqués dans la mise en place de nouveaux traitements sont encouragés à anticiper les risques et à solliciter le DPO dès la phase de réflexion du projet.

PARTAGE DES DONNÉES

> Partage des données personnelles

MEOGROUP peut être amené à partager certaines données personnelles avec des tiers dans le cadre de ses activités, uniquement dans les limites nécessaires à la réalisation des finalités définies et en conformité avec la réglementation en vigueur :

- Une ou plusieurs filiales de MEOGROUP pour des raisons opérationnelles, administratives ou commerciales,
- Les prestataires et sous-traitants intervenant pour le compte de MEOGROUP,
- Les partenaires et clients, lorsque cela est nécessaire à l'exécution des missions confiées ou à la gestion des relations contractuelles,
- Les autorités administratives et judiciaires, lorsque la loi l'exige ou dans le cadre de procédures légales.

Tout partage de données fait l'objet d'un encadrement contractuel strict afin d'assurer leur protection, notamment par l'intégration de clauses de confidentialité et, le cas échéant, par la mise en place d'accords spécifiques.

> Cas des transferts de données hors Europe

Dans le cadre de ses activités, MEOGROUP peut être amené à transférer des données personnelles en dehors de l'Espace Économique Européen (EEE). Ces transferts interviennent uniquement lorsque cela est nécessaire à la réalisation des finalités définies et dans le respect de la réglementation en vigueur.

Lorsque des données sont transférées hors de l'EEE, notamment vers des filiales du groupe, MEOGROUP met en place des garanties appropriées pour assurer leur protection.

Lorsque les destinataires des données sont situés dans un pays ne bénéficiant pas d'une décision d'adéquation de la Commission européenne, des garanties appropriées sont mises en place, telles que les clauses contractuelles types de la Commission européenne ou d'autres mécanismes reconnus permettant d'assurer un niveau de protection adéquat.

DROITS DES PERSONNES CONCERNÉES

Conformément aux lois applicables, chaque individu bénéficie de plusieurs droits (liste ci-dessous non exhaustive) relatifs à ses données. Ces droits visent à garantir la transparence, la sécurité et le contrôle de l'utilisation de ses informations personnelles.

1. **Droit d'accès** :
   Une personne a le droit de savoir si ses données personnelles sont traitées par MEOGROUP et, si tel est le cas, d'obtenir des informations détaillées sur les finalités du traitement, les catégories de données collectées, les destinataires des données, ainsi que la durée de conservation.

2. **Droit de rectification** :
   Une personne peut demander la correction de toute donnée personnelle la concernant détenue par MEOGROUP si elle la juge inexacte ou incomplète.

3. **Droit à l'effacement (ou droit à l'oubli)** :
   Une personne peut demander la suppression de ses données personnelles détenue par MEOGROUP lorsque celles-ci ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées, ou si elle retire son consentement lorsque ce dernier est la base légale du traitement.

4. **Droit d'opposition** :
   Une personne peut s'opposer, sans justification, à un traitement – exécuté par MEOGROUP – de ses données basées sur l'intérêt légitime. Dans certains cas, elle peut également s'opposer au traitement de ses données à des fins de prospection commerciale.

5. **Droit de retirer son consentement** :
   Une personne peut à tout moment retirer son consentement auprès de MEOGROUP, sans que cela n'affecte la légalité du traitement effectué avant le retrait.

PROCÉDURE POUR EXERCER LES DROITS DES PERSONNES CONCERNÉES

Afin d'exercer leurs droits relatifs à la protection des données personnelles, les personnes concernées doivent soumettre une demande écrite, en précisant le droit qu'elles souhaitent exercer :

- Soit par courrier électronique : dpo@meogroup-consulting.com,
- Soit en utilisant le formulaire présent dans la plateforme sur laquelle les données sont collectées,
- Soit par courrier postal :
  MEOGROUP - A l'attention du DPO
  27/33 Quai Alphonse LE GALLO
  92100 Boulogne-Billancourt

France.

La demande doit inclure les informations nécessaires pour permettre d'identifier clairement la personne concernée, telles que ses coordonnées et, si nécessaire, une copie de pièce d'identité.

Le DPO dispose d'un délai d'un mois à compter de la réception de la demande pour y répondre. En fonction de la complexité et du nombre de demandes, ce délai peut être prolongé de deux mois supplémentaires.

Si la demande est jugée infondée ou excessive, des frais peuvent être appliqués ou la demande peut être rejetée.

Si la personne concernée estime que ses droits ne sont pas respectés, elle peut saisir l'autorité de protection des données compétente.

SÉCURITÉ DES DONNÉES

LISTES DES MESURES TECHNIQUES ET ORGANISATIONNELLES

Les mesures techniques et organisationnelles sont décrites par pays et dans des documents séparés.

Les documents suivants sont également disponibles :

- Politique de Sécurité des Systèmes d'Information (PSSI),
- Charte Utilisateur du Système d'Informations,
- Politique de sauvegarde et de restauration des données,
- Politique de définition et de gestion des mots de passe,
- Politique de prêt de ressources informatiques et téléphoniques,
- Procédure de gestion des incidents traitant de données personnelles,
- Cartographies des solutions, des flux et de l'infrastructure,
- Charte administrateur,
- Politique de journalisation des accès aux solutions,
- Planning d'audits internes et externes.

GESTION DES VIOLATIONS DE DONNÉES

En cas de violation de données personnelles, une procédure spécifique est mise en œuvre afin d'en limiter les impacts et d'assurer la conformité aux obligations légales.

Toute suspicion ou identification d'une violation doit être signalée immédiatement au DPO. Une analyse est réalisée afin d'évaluer la nature, l'ampleur et les conséquences potentielles de l'incident.

Si la violation présente un risque pour les droits et libertés des personnes concernées, l'autorité de contrôle compétente sera notifiée dans un délai maximal de 72 heures à compter de sa découverte, conformément à la réglementation en vigueur. Lorsque le risque est élevé, les personnes concernées seront également informées dans les meilleurs délais.

Des mesures correctives et préventives sont mises en place pour remédier à la situation et éviter toute récurrence.

Un registre des incidents est tenu à jour pour assurer un suivi et une amélioration continue du dispositif de protection des données.

SENSIBILISATION ET FORMATION

MEOGROUP accorde une importance particulière à la sensibilisation et à la formation de ses collaborateurs en matière de protection des données personnelles et de cybersécurité.

Afin de renforcer la culture de la protection des données au sein de l'entreprise, nous avons mis en place un programme de cyber sensibilisation, permettant à chaque collaborateur de mieux comprendre les risques et d'adopter les bonnes pratiques.

Ce programme, détaillé dans un document séparé, comprend :

- Des formations régulières,
- Des ateliers de sensibilisation pour les nouveaux arrivants,
- Des vidéos pour expliquer simplement des grands concepts,
- Des webinaires pour approfondir les sujets principaux, expliquer les impacts et évaluer leur compréhension,
- Des études de cas pour sensibiliser les collaborateurs aux enjeux,
- Des tests, des exercices et simulations pour tester les réflexes,
- Des ressources et guides internes sur les bonnes pratiques en matière de confidentialité et de sécurité des données.

CONTACTS PRINCIPAUX

- Pour toute demande concernant la protection des données personnelles, veuillez contacter notre équipe dédiée à **dpo@meogroup-consulting.com**.

- Pour toute question ou préoccupation relative à la cybersécurité, veuillez contacter notre équipe dédiée à **cybersecurity@meogroup-consulting.com**.

- Pour toute réclamation, veuillez contacter notre équipe dédiée à **reclamation@meogroup-consulting.com.**

- Pour toute assistance ou demande informatique, veuillez contacter notre équipe dédiée à **si@meogroup-consulting.com**.