HAVAS GROUP

CONFORMITÉ RGPD

SOMMAIRE

INTRODUCTION ET OBJECTIF

Le règlement général sur la protection des données (RGPD) à caractère personnel du 27 avril 2016 sera applicable le 25 mai 2018. Ce règlement abroge la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

L'un des objectifs du RGPD (considérant 7) est de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur.

POUR CE FAIRE, LE RGPD VISE À :

HARMONISER les réglementations
RENFORCER le droit des personnes situées sur le territoire de l'Union Européenne avec l'introduction de nouveaux concepts
RESPONSABILISER l'ensemble des acteurs (responsable de traitement et sous-traitant), tant au niveau des obligations leur incombant spécifiquement que par le champ d'application territorial
CRÉDIBILISER la régulation

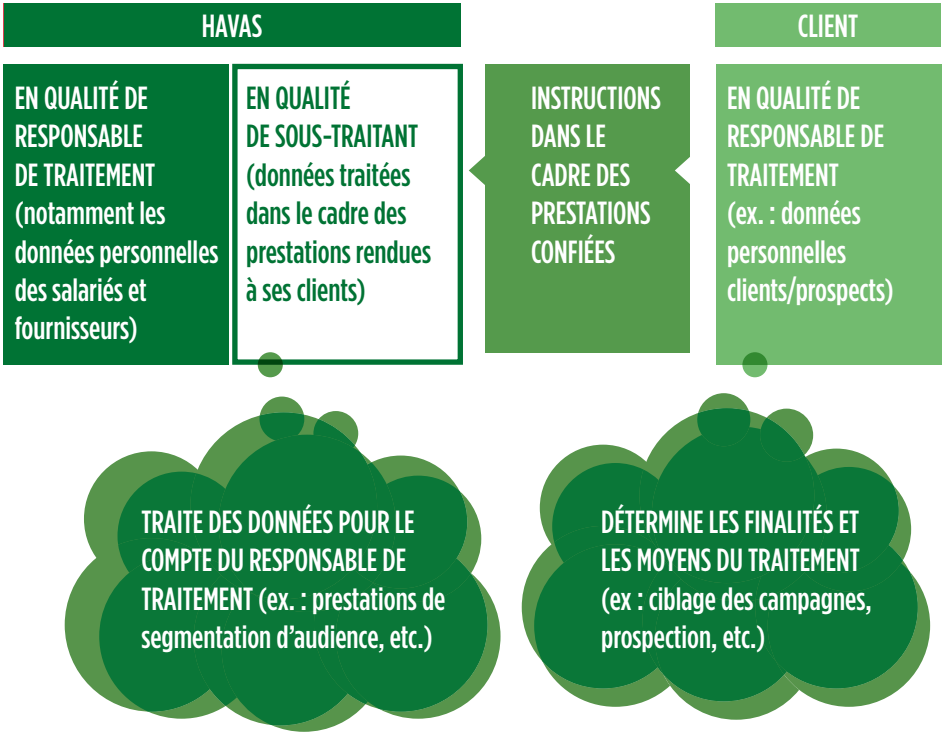
Le RGPD opère un véritable changement de paradigme qui est une réelle opportunité pour chacun d'améliorer les process et favoriser la collaboration des acteurs traitant des données personnelles.

L'objectif de cette présentation est de décrire les dispositions mises en œuvre par les entités du Groupe Havas, en leur qualité de sous-traitant, pour se conformer au RGPD.

Les mesures décrites dans cette présentation ne sont pas exhaustives et sont soit déjà mises en œuvre soit en cours de mise en œuvre.

LES GRANDS PRINCIPES DU RGPD

POSITIONNEMENT DES ENTITÉS DU GROUPE HAVAS



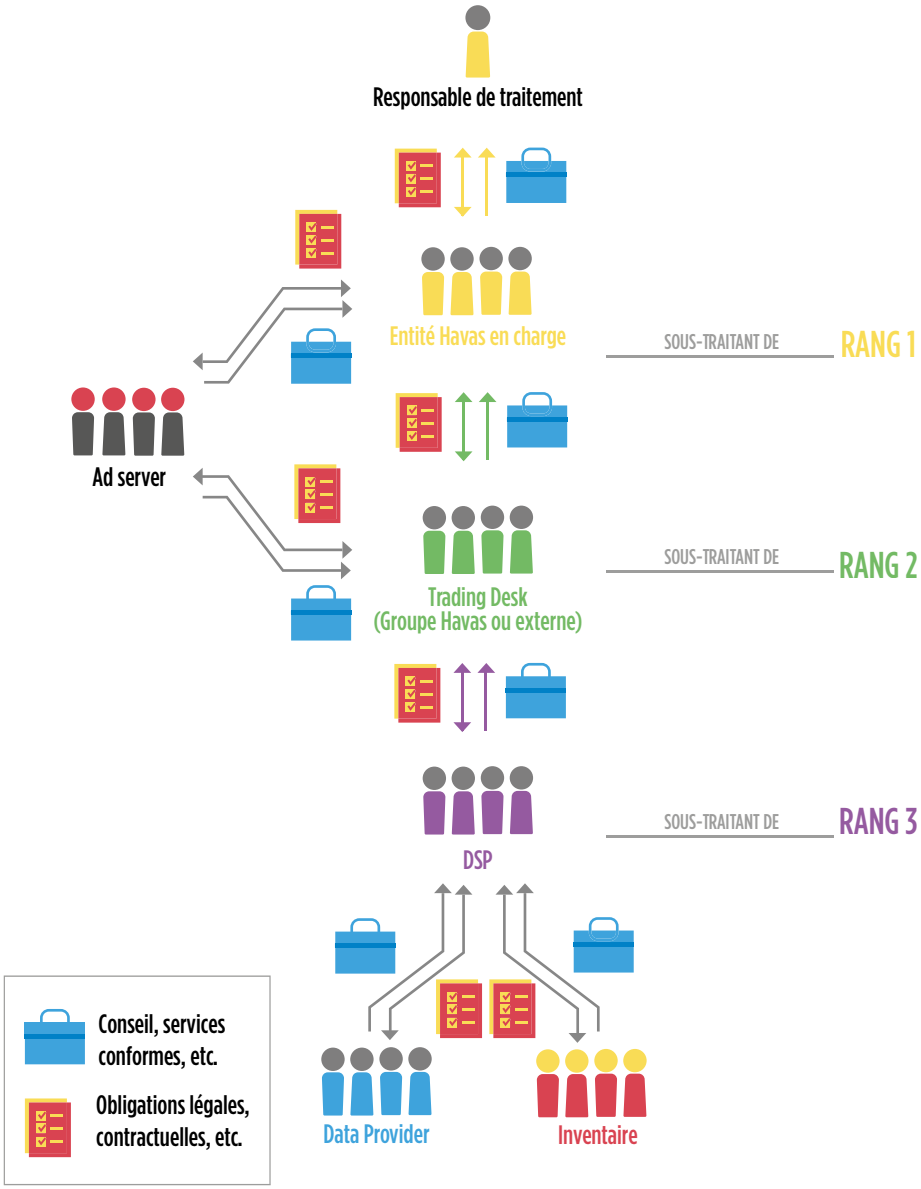
ÉCOSYSTÈME DE LA CHAÎNE DE SOUS-TRAITANCE

Principalement dans le cadre des services rendus par les entités du groupe Havas, ces dernières agissent en qualité de sous-traitants de premier rang et peuvent faire appel à des sous-traitants de second rang et ultérieurs.

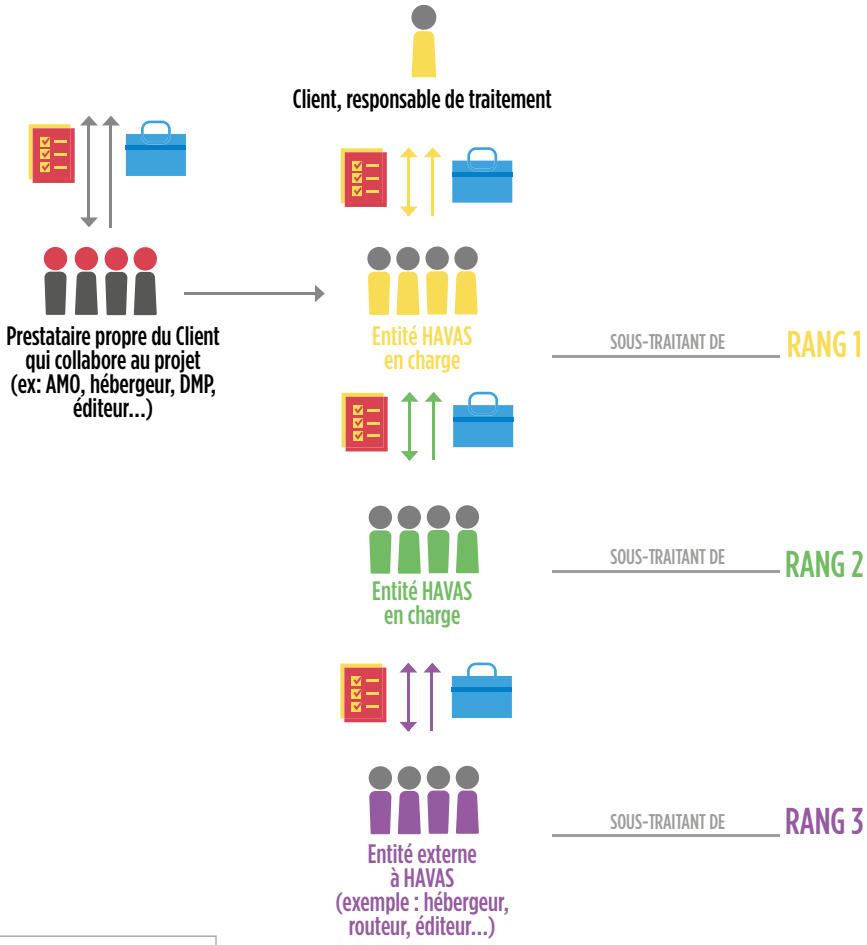
L'ensemble des acteurs de la chaîne sont responsables, que ce soit le responsable de traitement ou l'ensemble des sous-traitants de la chaîne. Les responsabilités de chacun doivent être définies précisément et contractuellement afin de limiter les risques.

La conformité des entités Havas est essentielle mais n'est pas suffisante. Celle des autres acteurs intervenant dans la chaîne tant au niveau du responsable de traitement que de l'ensemble des sous-traitants est déterminante.

EXEMPLE 1 - MÉDIA



EXEMPLE 2 - DÉVELOPPEMENT



UNE NÉCESSAIRE CONFORMITÉ DE L'ENSEMBLE DE L'ÉCOSYSTÈME

Pour chaque traitement, l'ensemble des intervenants de la chaîne de traitement, du responsable de traitement jusqu'au sous-traitant de dernier rang, doivent traiter les données à caractère personnel (DCP) en conformité avec la réglementation applicable :

LE CLIENT, responsable de traitement et ses sous-traitants directs distincts de l'entité Havas

LE SOUS-TRAITANT HAVAS ET SES SOUS-TRAITANTS ULTÉRIEURS, qu'ils fassent partie du groupe Havas ou non

La conformité implique nécessairement la coopération de l'ensemble des acteurs de la chaîne.

LES GARANTIES APPORTÉES PAR HAVAS DANS SON RÔLE DE SOUS-TRAITANT

Des mesures de sécurité appropriées

Des engagements contractuels

Une sous-traitance approuvée et maîtrisée

LES ENGAGEMENTS CONTRACTUELS DE HAVAS ET LA SOUS-TRAITANCE ULTÉRIEURE

Les engagements de l'entité Havas au titre du contrat le liant à son client et repris dans le contrat qui le lie à un sous-traitant ultérieur approuvé par le Client d'HAVAS, sont :

- Ne **traiter** les DCP que sur instruction documentée du responsable de traitement, y compris en ce qui concerne le transfert hors Union Européenne. Dans ce dernier cas, les mesures appropriées devront être prises.

- **Veiller** à ce que les personnes autorisées à traiter les DCP s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

- **Prendre** toutes les mesures de sécurité requises en vertu de l'article 32 du RGPD.

- **Recruter** un sous-traitant qu'avec l'accord préalable et répercuter l'ensemble des obligations issues de l'article 28 du RGPD et du contrat Client.

- **Tenir compte** de la nature du traitement, aider le responsable de traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes des personnes concernées.

- **Aider** le responsable de traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD (sécurité, notification et communication des violations de données, analyses d'impact et consultation préalable de l'autorité de contrôle) compte tenu de la nature du traitement et des informations à sa disposition.

- **Supprimer** toutes les DCP ou les restituer au responsable de traitement, et détruire toutes les copies existantes selon le choix du responsable de traitement.

- **Mettre** à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audit.

- **Notifier** le responsable de traitement si le sous-traitant considère qu'une instruction est non conforme à la règlementation.

LA SÉCURITÉ (ARTICLE 32 DU RGPD)

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

    a) la pseudonymisation et le chiffrement des données à caractère personnel.

    b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

    c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique.

    d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

La collaboration entre l'agence, le Client et les intervenants extérieurs du Client en matière de sécurité est essentielle. La sécurité doit être prise en compte dès la conception (privacy by design) et par défaut. Le principe de minimisation (par exemple, ne traiter que les données strictement nécessaires à la finalité du traitement) participe à la sécurité et une collaboration étroite est là encore nécessaire.

LES MESURES PRISES PAR LE GROUPE HAVAS

POUR SATISFAIRE SES IMPÉRATIFS

Le contrat qui définit les missions de l'agence et les obligations de chacune des parties en matière de traitement de DCP (respect des engagements prévus par la réglementation, sécurité, confidentialité...)

L'annexe au contrat, au bon de commande ou devis qui définit pour chaque traitement : l'objet et la durée du traitement, la nature et la finalité du traitement, le type de DCP et les catégories de personnes concernées.

La charte de protection des DCP :

- Politique de sécurité, Plan d'Assurance Qualité (PAQ), Service Level Agreement (SLA)
- Politique de confidentialité
- Politique de notification des violations
- RACI si nécessaire

Des instructions du client claires, précises et documentées

PARTENAIRES ET SOUS-TRAITANTS DES ENTITÉS DU GROUPE HAVAS

Havas fait signer à chacun de ses fournisseurs un contrat reprenant les points évoqués ci-avant, et les fournisseurs actuels doivent s'engager sur une Charte de protection des données afin que leurs engagements soient mis à jour avec le RGPD.

Transfert

Les entités du Groupe Havas font appel uniquement, avec l'accord préalable du client à des prestataires et des sous-traitants situés sur le territoire de l'Union Européenne ou situés dans un pays reconnu par la Commission Européenne comme offrant un niveau de protection adéquat (exemple : Privacy Shield).

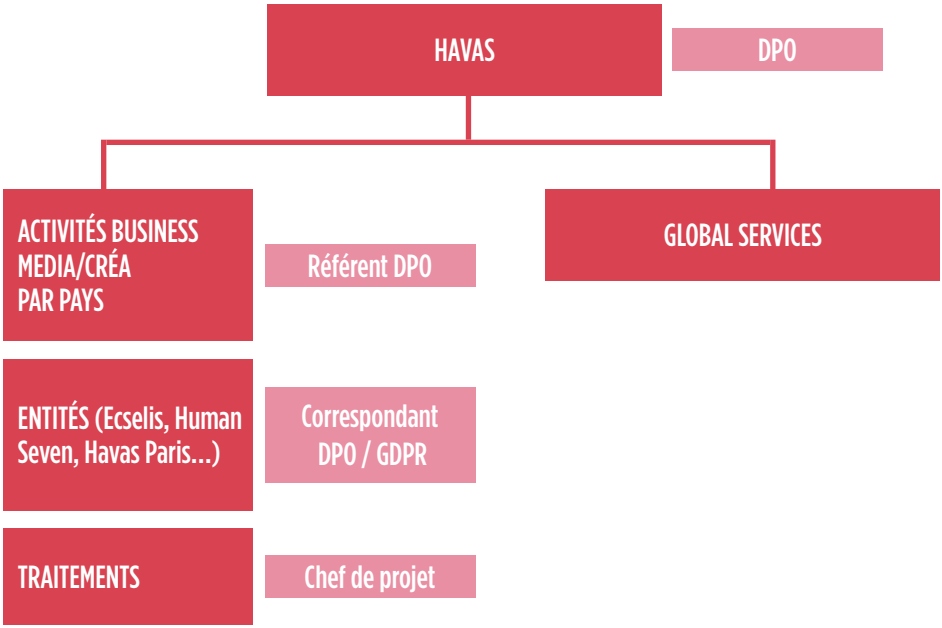
En dehors de ces cas, si une entité du groupe Havas doit faire appel, en accord avec le responsable du traitement, à un sous-traitant situé hors Union Européenne et qui n'est pas considéré comme présentant un niveau de protection adéquate, des Clauses Contractuelles type selon le modèle établi par la Commission Européenne seront signées entre l'entité Havas et le ou les sous-traitants concernés.

MESURES TECHNIQUES ET ORGANISATIONNELLES - GOUVERNANCE

DPO (Data Protection Officer) Daniele Nguyen

Rôle (article 37 à 39)

- Informer et conseiller l'ensemble des entités du groupe Havas
- Contrôler le respect du RGPD par les entités du groupe Havas
- Conseiller sur l'analyse d'impact
- Coopérer avec l'autorité de contrôle



MESURES TECHNIQUES ET ORGANISATIONNELLES – SÉCURITÉ

Les moyens IT pour assurer la sécurité

Havas a organisé la gouvernance de la sécurité des systèmes d'information avec un service central et un directeur Sécurité qui définissent les standards à appliquer dans toutes les agences du groupe. Chaque service IT local a charge de faire appliquer ces politiques standards. Des contrôles en découlent et sont pratiqués régulièrement.

En France, Havas IT, qui fournit les moyens informatiques pour les agences du groupe Havas, assure l'application des politiques du groupe.

C'est l'ensemble de ces politiques (ou règles) et leur application qui constitue la sécurité des données personnelles (ou non) de l'entreprise et de nos clients.

Quelques sujets majeurs se distinguent dans les politiques de sécurité obligatoires du groupe que nous listons ici.

Sécurité physique

La sécurité physique et environnementale protège l'information, l'infrastructure des systèmes d'information et les installations contre les menaces physiques et environnementales. L'accès physique aux zones de traitement de l'information et à leur infrastructure (communications, électricité et environnement) doit être contrôlé pour prévenir, détecter et minimiser les effets de l'accès involontaire à ces zones (accès non autorisé à l'information ou perturbation du traitement de l'information).

Le groupe Havas traite systématiquement ces questions liées au périmètre de sécurité physique, aux contrôles d'accès physique, aux conditions de travail, à la sécurisation des bureaux, aux centres de données, à la sécurité de l'équipement et aux contrôles généraux au travers d'un ensemble de politiques qui sont obligatoirement appliquées aux ressources concernant les agences du groupe Havas et les données de ses clients.

En pratique cela signifie par exemple que les centres d'hébergement de données ou serveurs font l'objet d'accès physiques restreints et contrôlés.

Sécurité logique
Accès des employés aux systèmes informatiques

Un ensemble de règles régit l'accès d'une personne aux ressources informatiques parmi lesquelles (liste non exhaustive) :

- Les agences Havas doivent identifier et authentifier tous les utilisateurs avant d'accorder l'accès (uniquement) aux systèmes appropriés.

- Chaque utilisateur doit posséder ses propres identifiants qui ne sont ni échangeables ni communicables.
- Une politique de mots de passe complexe est imposée avec rotation.
- L'usage des programmes et les accès aux données sont restreints aux personnes autorisées uniquement et selon leur mission.
- Les propriétaires/responsables des données doivent vérifier les listes d'accès une fois par an au minimum.
- La révocation des accès doit avoir lieu par Havas IT dès que possible.
- Les moyens de contrôle et d'accès aux données prennent également en compte les différents types de terminaux mis à disposition.

Gestion de la sécurité de réseaux

Les réseaux du groupe Havas sont interconnectés et protégés d'Internet par des équipements de type pare-feu. Ils suivent une norme de sécurité standardisée dans le groupe et sont gérés uniformément. Ils doivent être tenus à jour des mises à jour éditeur et répondent à des règles de sécurité intrinsèques (gestion des mots de passe d'administration par exemple).

Les réseaux restent segmentés et protégés à différents niveaux par ces équipements.

Les réseaux doivent rester séparés logiquement et les échanges entre eux limités aux besoins strictement nécessaires.

Les éléments réseaux d'extrémité et les Wi-Fi répondent également à des normes groupe de sécurité.

Autres éléments de sécurité IT du groupe

Les éléments de type serveurs, stations de travail et éléments réseaux font l'objet d'une politique de mises à jour éditeur stricte.

Les éléments de type serveurs et stations de travail font l'objet d'une politique normée de logiciel antivirus.

Les disques locaux des stations de travail sont cryptés.

Une politique de classification des données vient en support des restrictions d'accès par les utilisateurs ou tiers.

Des normes de transmissions de données et leur chiffrement sont clairement établis et les outils pour ce faire restreints.

MESURES TECHNIQUES ET ORGANISATIONNELLES - FORMATION

SENSIBILISATION ET FORMATION À DESTINATION DES PERSONNES DES DIFFÉRENTES ENTITÉS QUI TRAITENT DE LA DONNÉE À CARACTÈRE PERSONNEL

FORMATION À L'ENSEMBLE DES COLLABORATEURS DU GROUPE HAVAS DANS LE MONDE SOUS FORME DE E-LEARNING

FORMATION APPROFONDIE À DESTINATION DE CERTAINS SERVICES/ACTIVITÉS/ENTITÉS EN FONCTION DE LEUR PROBLÉMATIQUE

HAVAS UNIVERSITY

ACCOUNTABILITY

Plateforme technologique One Trust

L'outil One Trust permet de réaliser :
- Le registre de traitement et le data mapping (article 30)
- L'étude d'impact sur la vie privée (article 35)
- Le suivi de la conformité des sous-traitants

OneTrust
Privacy Management Software
Plateforme technologique (Privacy Shield)

→

Traçabilité
Documentation
GAP analysis

Le registre de traitement du sous-traitant (art 30)

Chaque sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- **Le NOM ET LES COORDONNÉES du ou des sous-traitants et de chaque responsable de traitement pour le compte duquel le sous-traitant agit ainsi que le cas échéant, les noms et les coordonnées du représentant du responsable de traitement ou du sous-traitant et celles du DPO.**
- **Les CATÉGORIES DE TRAITEMENTS effectuées pour le compte de chaque responsable de traitement.**
- **Le cas échéant les TRANSFERTS de DCP vers un pays tiers**
- **Dans la mesure du possible, une DESCRIPTION GÉNÉRALE des mesures de sécurité techniques et organisationnelles.**

NOTIFICATION DES VIOLATIONS

LES SOLUTIONS D'ACCOM-PAGNEMENT

BESOIN D'UN ACCOMPAGNEMENT ?

DBI accompagne les marques pour **valoriser une data activable, pertinente et efficace sur le business,** pour une **expérience utilisateur personnalisée.**

Un **accompagnement complet**, de la définition de roadmap **jusqu'à la mise en œuvre concrète** dans les **campagnes marketing dans le respect du RGPD.**

Programme technologique dédié au RGPD

Diagnostic

RECENSEMENT DATA

Identifier les données personnelles dans les traitements des données marketing digitales

Catalogue des traitements et des données digitales

DATA MAPPING

Identifier les acteurs impliqués dans les traitements de données, leur responsabilité, le lieu de stockage et les transferts des données

Cartographie des acteurs et mapping des transferts

COOKIE & CRM COMPLIANCE

Identifier les cookies collectés et les données CRM et vérifier le recueil des consentements nécessaires

Cookie & CRM notice checklist

DBi DATA BUSINESS INTELLIGENCE

OneTrust Privacy Management Software

Programme technologique dédié au RGPD

Recommandations

CLEANING	RISK EVALUATION	PRIORISATION
Nettoyage des traitements de données et des technologies de collecte non utiles	Identification d'un niveau de risque sur les traitements des données personnelles (recueil du consentement, traitements géographiques, durée de conservation)	Identification et priorisation des chantiers selon les risques estimés en collaboration avec votre DPO et les acteurs impliqués
Optimisation des tags	Catégorisation des risques	Plan d'action

DBi DATA BUSINESS INTELLIGENCE

Contact DBi : rgpd.dbi.io

Pour Ekino, MFG Labs, Fullsix

Diagnostic et développement technique de mise en œuvre du RGPD

mfg labs

dc@mfglabs.com

ekino.

dc@ekino.com

fullsix

agence@fullsix.com

DES QUESTIONS ?

DPO

Daniele Nguyen

dpo@havas.com

Éditeur :
Havas - 29-30, Quai de Dion-Bouton
92800 PUTEAUX

Document gratuit - ne peut être vendu

CONFORMITÉ
RGPD

HAVAS
GROUP

HAVAS
GROUP

CONFORMITÉ RGPD