

Accord-cadre relatif à la fourniture et distribution d'habillement, d'accessoires et d'équipements, destinés aux personnels de la Direction Générale des Douanes et des Droits Indirects (DGDDI)

**Annexe 2
Traitement des données à caractère personnel**

1. OBJET de l'annexe

La présente annexe a pour objet de définir :

- les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte de la DGDDI les opérations de traitement de données à caractère personnel définies au sens du RGPD, et décrites **en annexe 2.1** ;
- les obligations de la DGDDI vis-à-vis du titulaire.

2. OBLIGATIONS DU TITULAIRE VIS-A-VIS DE LA DGDDI

Conformément à la réglementation en vigueur applicable au traitement des données à caractère personnel et, en particulier, le règlement général sur la protection des données (règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016),

Le titulaire s'engage à :

- traiter les données à caractère personnel uniquement pour la ou les seule(s) finalité(s) figurant **en annexe 2.1** ;
- traiter les données à caractère personnel conformément aux instructions de la DGDDI définies **en annexe 2.1**. Si selon le titulaire l'une de ces instructions constitue une violation du RGPD, il en informe immédiatement la DGDDI. En outre, si le titulaire est tenu de procéder à un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis, il doit informer la DGDDI de cette obligation avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
- garantir la confidentialité des données à caractère personnel traitées dans le cadre du marché ;
- prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut ;
- tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de la DGDDI ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du marché soient soumises à une obligation de confidentialité et soient formées en matière de protection des données à caractère personnel ;

- aider la DGDDI, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits d'accès et de rectification, voire d'opposition ou de limitation vis-à-vis du traitement ;
- apporter tout son concours à la DGDDI dans l'élaboration du Dossier de conformité du traitement à la réglementation sur la protection des données (« DC-POD ») soumis à validation du délégué ministériel à la protection des données (« DPD ») et le cas échéant à consultation de la Commission Nationale de l'Informatique et des Libertés (CNIL), autorité de contrôle ;
- apporter le cas échéant tout son concours à la DGDDI dans la réalisation de l'Analyse d'impact relative à la protection des données (« PIA ») soumise à validation du DPD et le cas échéant pour la réalisation de la consultation préalable de la CNIL ;
- aider la DGDDI à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD, compte tenu de la nature du traitement et des informations à la disposition du titulaire ;
- à la demande de la DGDDI, supprimer ou renvoyer à celui-ci toutes les données à caractère personnel au terme de la prestation de service relatifs au traitement, et détruire les copies existantes ;
- notifier à la DGDDI toute violation de données à caractère personnel dès le moment où elle en a connaissance et au plus tard vingt-quatre (24) heures après la découverte de la violation ;
- mettre à disposition de la DGDDI toutes les informations nécessaires pour démontrer le respect des obligations qui incombent au titulaire et pour permettre la réalisation d'audits, y compris des inspections, par le responsable de traitement opérationnel, et contribuer à ces audits.
- informer la DGDDI de toute opération de contrôle menée par la CNIL auprès du titulaire, mettre à disposition de la DGDDI toutes les informations utiles dans le cadre du contrôle et prendre toutes mesures nécessaires afin de faciliter la tâche de l'autorité de contrôle ;
- informer la DGDDI préalablement et par écrit si elle décide de confier la réalisation d'une partie du traitement à un tiers (dit « sous-traitant ultérieur ») pour mener des activités de traitement spécifiques ;
- de manière générale, fournir à la DGDDI, sur sa demande, toute information relative au traitement.

Sous-traitance

Le titulaire peut confier la réalisation d'une partie du traitement à un tiers (ci-après « le sous-traitant »), pour mener des activités de traitement spécifique. Dans ce cas, il informe préalablement et par écrit la DGDDI de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du Sous-traitant et les dates du contrat de sous-traitance. La DGDDI dispose d'un délai de quinze (15) jours à compter de la date de réception de cette information pour présenter par écrit ses objections motivées. Cette sous-traitance ne peut être effectuée que si la DGDDI n'a pas émis d'objection pendant ledit délai.

Les sous-traitants intervenant dans l'exécution des prestations à la date de notification de la présente annexe demeurent autorisés à réaliser les traitements qui leur ont été confiés.

Le titulaire s'assure que le sous-traitant présente les mêmes garanties quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD. Si le sous-traitant ne remplit pas ses obligations en matière de protection

des données à caractère personnel, le titulaire demeure pleinement responsable à l'égard de la DGDDI de l'exécution par le sous-traitant de ses obligations.

Le titulaire peut librement confier tout ou partie de la réalisation du traitement à toute société de son groupe qu'il contrôle ou qui le contrôle au sens de l'article L 233-3 du Code de commerce. Il doit en informer préalablement la DGDDI.

Droit d'information des personnes concernées

Il appartient à la DGDDI de fournir l'information requise par le RGPD aux personnes concernées par les opérations de traitement, au moment de la collecte des données à caractère personnel.

Exercice des droits des personnes

Dans la mesure du possible, le titulaire doit aider la DGDDI à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données à caractère personnel, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent directement auprès du titulaire des demandes d'exercice de leurs droits, le titulaire doit adresser ces demandes dès réception par courrier électronique à la DGDDI.

Notification des violations de données à caractère personnel

Une violation de données est une faille de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à ces données.

Le titulaire notifie à la DGDDI toute violation de données à caractère personnel dès le moment où il en a connaissance et au plus tard vingt-quatre heures (24) après la découverte de la violation. La notification est réalisée par tous moyens écrits y compris les correspondances électroniques. Cette notification est accompagnée de toute documentation utile afin de permettre à la DGDDI, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente dans les conditions prévues par l'article 33 du RGPD.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le titulaire propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

La notification à l'autorité de contrôle est réalisée par la DGDDI dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en

question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Si l'autorité de contrôle commande la communication de la violation de données à la personne concernée, la DGDDI réalise cette communication auprès des personnes concernées lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. Cette communication a lieu dans les meilleurs délais.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données des ministères économique et financier ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le titulaire propose de prendre pour remédier à la violation y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Mesures de sécurité

Le titulaire s'engage à mettre en œuvre les mesures de sécurité arrêtées d'un commun accord avec la DGDDI et définies **en annexe 2.2**.

Sort des données à caractère personnel à l'issue du marché

A l'issue du marché, le titulaire s'engage :

- à renvoyer toutes les données à caractère personnel à la DGDDI. Cette restitution pourra, le cas échéant, faire l'objet d'une facturation,
- et à détruire toutes les copies existantes dans ses systèmes d'information, sauf si la conservation des données à caractère personnel est exigée en vertu du droit de l'Union ou de la législation interne.

Registre des catégories d'activités de traitement

Le titulaire déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de la DGDDI, comprenant :

- le nom et les coordonnées d'un représentant de la DGDDI, des éventuels sous-traitants, et le cas échéant, du référent du délégué à la protection des données, lequel est mentionné **en annexe 2.1**;
- les catégories de traitements effectués pour le compte de la DGDDI ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées ;

- dans la mesure du possible une description générale des mesures de sécurité techniques et organisationnelles telles que visées **en annexe 2.2**.

Documentation / audit

Le titulaire met à la disposition de la DGDDI les informations nécessaires pour démontrer le respect de ses obligations prévues à l'article 28 du RGPD et pour lui permettre de réaliser des audits, y compris des inspections, aux frais de la DGDDI. L'audit sera mené par la DGDDI ou un auditeur qu'il aura mandaté, non-concurrent du titulaire, et soumis à une obligation de confidentialité.

La DGDDI s'engage à notifier avec un préavis minimum de quinze (15) jours au titulaire tout audit, en lui communiquant notamment l'objet de la mission, la durée envisagée, et le nom du ou des auditeur(s).

Le titulaire pourra opposer un refus d'auditeur pour préserver ses intérêts légitimes.

Le titulaire mettra en place les moyens raisonnables pour permettre à l'auditeur de mener à bien son audit. Les opérations d'audit et les demandes d'information devront être effectuées pendant les heures normales d'ouverture du Sous-traitant et ne devront pas perturber le bon fonctionnement des activités de ce dernier.

Au titre de cette assistance fournie à la DGDDI par le titulaire, ce dernier interviendra sans frais supplémentaire pour la DGDDI dans la limite de deux (2) jours/homme par an. Toute mobilisation complémentaire de ressource du titulaire pour cette assistance sera facturée à la DGDDI.

Un exemplaire du rapport d'audit sera remis gracieusement au titulaire. Les Parties examineront de bonne foi ce rapport, et identifieront, le cas échéant, les actions qui devront être engagées par l'une ou l'autre des Parties pour mettre en œuvre les décisions.

3. OBLIGATIONS DE LA DGDDI VIS-A-VIS DU TITULAIRE

La DGDDI s'engage à respecter le RGPD et toute norme législative ou réglementaire applicable aux données à caractère personnel traitées, et notamment à :

- respecter le principe de limitation des données à caractère personnel nécessaires au regard des finalités de traitement. Par conséquent, la DGDDI s'engage à anonymiser ou pseudonymiser autant que possible ses données à caractère personnel, et en tout état de cause à ne confier au titulaire que les données à caractère personnel strictement nécessaires à l'exécution des prestations,
- s'assurer que les traitements et leurs finalités sont conformes au RGPD,
- fournir au titulaire la description du traitement et les instructions associées, qui figurent toutes deux **en annexe 2.1**. Toute modification de l'Annexe devra faire l'objet d'un avenant au marché.
- veiller, au préalable et pendant toute la durée du traitement, au respect par le titulaire des obligations prévues par le RGPD, dont notamment les dispositions de l'article 25 dudit règlement ;
- fournir l'information requise par le RGPD aux personnes concernées par les opérations de traitement, au moment de la collecte des données à caractère personnel ;
- superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire, selon les conditions et modalités visées ci-dessus (cf. « Documentation / audit »).

ANNEXE 2.1

DESCRIPTION DU TRAITEMENT

Le titulaire est autorisé à traiter pour le compte de la DGDDI les données à caractère personnel nécessaires pour fournir les prestations objet du marché.

La DGDDI déclare que :

- La nature des opérations réalisées sur les données à caractère personnel est **leur exploitation dans le cadre de la passation de commandes d'habillement auprès de nos fournisseurs.**
- La ou les finalité(s) du traitement sont **de permettre aux agents des douanes de réaliser des commandes d'effets d'habillement et de suivre leur livraison.**
- Les données à caractère personnel traitées sont **les noms, prénoms, grades, services d'affectation et numéros de matricule des agents.**
- Les catégories de personnes concernées sont **tous les agents des douanes.**

- Le DPO de la DGDDI est :

Le Délégué à la protection des données des ministères économique et financier
Délégation aux systèmes d'information
139 rue de Bercy. Télédocus 322 Paris CEDEX 12
le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr

- Un référent est désigné pour la DGDDI :

Direction générale des douanes et droits indirects
Bureau JCF1 - Bureau des affaires juridiques et contentieuses
11 rue des Deux Communes, 93100 MONTREUIL
protectiondesdonneesdouane@douane.finances.gouv.fr

Pour l'exécution des Prestations objet du marché, la DGDDI met à la disposition du titulaire les informations et instructions nécessaires suivantes :

NOM

PRENOM

Site de livraison

Article fournisseur

Libellé service

Adresse de livraison

Horaires d'ouverture du service

La DGDDI s'engage à donner au titulaire des instructions et finalités de traitement de ses données à caractère personnel conformes au RGPD.

La DGDDI devra notifier au titulaire toute modification du traitement, cette modification devra faire l'objet d'un avenant.

MESURES DE SECURITE TECHNIQUES ET ORGANISATIONNELLES

Conformément aux prescriptions de l'article 32 du RGPD, le titulaire s'engage à mettre en œuvre les mesures de sécurité suivantes, validées par la DGDDI :

- Pour ses Systèmes d'Information, une PSSI (Politique de Sécurité des Systèmes d'Information) conforme à la Norme ISO/CEI 27001 ;
- Les mesures techniques et organisationnelles liées aux prestations objet de l'annexe, en conformité avec le RGPD et définies dans un Plan d'Assurance Sécurité (PAS) validé par les parties.

Le PAS précisera, notamment :

- les intervenants, les mesures organisationnelles, et les instances de gouvernance ;
- les modalités de stockage et de chiffrement (ou non) associés sur les environnements du titulaire, si différents des règles de la Politique de Sécurité du Groupe, et en conformité avec la classification définie pour le Contrat ;
- les mesures de sécurisation des échanges (chiffrement des liaisons, des flux, des e-mails...);
- les mesures liées aux accès des utilisateurs du titulaire (authentification, revues des habilitations...);
- les procédures d'intervention (support, consultation, suppression...);
- les procédures de gestion et de remontée des incidents sur les données à caractère personnel ;
- l'anonymisation ou la pseudonymisation des données à caractère personnel avant transmission au titulaire, si nécessaire aux prestations, ainsi que les éventuels cas de dérogation et la manière de les traiter.