

DIRECTIVES VISANT A RENFORCER LA COOPERATION ET L'ECHANGE D'INFORMATIONS ENTRE LES AUTORITES DOUANIERES ET LES AUTORITES FISCALES AU NIVEAU NATIONAL

V. Elaboration d'un protocole d'accord (PDA)

ii. Inde



Administration centrale des douanes et accises (CBEC)

Politique de partage des données

Février 2015

Table des matières

1.	Introduction	4
2.	Le besoin d'une politique de partage des données	4
2.1	Situation actuelle	4
2.2	Le besoin d'une politique	5
2.3	Portée et champ d'application	6
3.	La catégorisation des données	7
3.1	Données sensibles	7
3.2	Données non sensibles	10
4.	la catégorisation des utilisateurs	11
4.1	Mandaté par Statut.....	11
4.2	Autres agences gouvernementales	11
4.3	Organismes de recherche, commissions, etc.....	12
5.	Catégorisation des demandes et modalités de partage des données.....	13
5.1	Demandes ponctuelles	13
5.2	Échanges structurés de données identifiées	13
6.	Financement du partage de données.....	14
7.	Stockage et conservation des données	14
8.	Clause de réciprocité	14
9.	Clause de sauvegarde	14
10.	Annexe A : Échange actuel de données avec des agences externes	16
11.	Annexe B : Échange actuel de données avec des agences internes	20
12.	Annexe C : ISO 27001/27002	27
13.	Annexe D : Protocoles de connectivité informatique Mise en place de l'échange de données	31
14.	Annexe E : Modèle de demande	34
15.	Annexe F : Procédure proposée de partage des données.....	36
16.	Annexe G : Projet de Protocole d'accord	38
17.	Annexe H : Définitions.....	46

1. Introduction

Les données sont universellement reconnues comme une précieuse ressource dont la gestion doit en exploiter au maximum la valeur. La plupart des données sont aujourd'hui conservées et échangées par voie électronique, ce qui facilite les échanges tout en exacerbant le besoin d'un mécanisme d'échange structuré et sécurisé. La Politique nationale de partage et d'accessibilité des données (*National Data Sharing and Accessibility Policy, NDSAP*) de l'Inde stipule **notamment** que les principes sur lesquels doit reposer le partage et l'accessibilité des données sont l'ouverture, la flexibilité, la transparence, la protection de la propriété intellectuelle, la responsabilité formelle, le professionnalisme, l'interopérabilité, la qualité, la sécurité, l'efficacité, la responsabilité, la durabilité et le respect de la vie privée. Grâce à des fonds publics, de grands volumes de données sont générés par diverses organisations et institutions à travers le pays et peuvent être utilisées à des fins scientifiques, économiques et de développement.

2. Le besoin d'une politique de partage des données

2.1 Situation actuelle

L'Administration centrale des douanes et accises (*Central Board of Excise and Customs, CBEC*) dispose d'une vaste base de données de contribuables en matière de douanes, d'accise centrale et de services fiscaux. La Direction des Systèmes (*Direction of Systems, DoS*), CBEC détient ces données dans ses systèmes informatiques en qualité de dépositaire. Les données transactionnelles en ligne relatives aux douanes, à l'accise centrale et aux services fiscaux se trouvent dans les applications commerciales respectives (ICES, ACES, ICEGATE, etc.). La centralisation de son infrastructure informatique unifiée a également permis au CBEC de créer un entrepôt de données d'entreprises (*Enterprise Data Warehouse, EDW*) activement mis à profit pour répondre aux demandes de données des agences internes et externes.

Des agences externes ont demandé à ce que les données recueillies grâce à des fonds publics soient mises à la disposition de tous pour alimenter un débat rationnel, améliorer la prise de décision, contribuer à la formulation de politiques et répondre aux besoins de la société civile.

En Inde, ces données sont actuellement partagées de différentes manières et à travers diverses modalités avec plusieurs agences internes et externes. L'application ICEGATE de la CBEC sert d'interface pour fournir des données transactionnelles douanières à des agences telles que la Direction générale du commerce extérieur (DGFT), la Direction générale de l'information et des statistiques commerciales (DGCIS), la *Royal Bank of India* (RBI), etc.

Les données de l'Entrepôt de données d'entreprises sont de plus en plus utilisées pour répondre à des questions du Parlement et encadrer les réponses apportées aux demandes reçues en vertu de la loi sur le droit à l'information (*Right to Information*, RDI). Les détails de ces échanges avec des agences externes et internes en Inde sont repris aux Annexes A et B, respectivement.

Les données sont partagées avec des entités externes au moyen de l'une des méthodes suivantes :

1. via les adresses électronique officielles ou gouvernementales ;
2. via un protocole de transfert de fichiers sécurisé (*Secure file transfer protocol*, SFTP), surtout lorsque le fichier de données est volumineux et qu'il ne peut pas être envoyé en pièce jointe ;
3. via un Réseau privé virtuel (*Virtual Private Network*, VPN) pour certains utilisateurs externes approuvés dans le cas de rapports préapprouvés.

2.2 Le besoin d'une politique

En sa qualité de dépositaire, la CBEC conserve des données fiscales indirectes. Comme indiqué plus haut, les demandes de données provenant d'utilisateurs externes ont considérablement augmenté. Depuis 2011, la CBEC a par ailleurs adopté la norme ISO 27001 relative à la sécurité de l'information, pour laquelle elle est auditée chaque année par l'organisme *Standards Testing Quality and Certifications*, qui relève du ministère de la Technologie de l'Information et de la Communication. Cette norme révisée en 2013 se concentre sur le domaine précis de la sécurité des communications, dans lequel des directives strictes ont été fixées quant au transfert d'informations au sein des organisations et avec toutes les entités externes. L'extrait concerné se trouve à l'annexe C.

Il doit être replacé dans le contexte de l'essor des demandes de données, alimenté par une conscience croissante de la valeur et des avantages que celles-ci représentent. Elles permettent notamment :

1. de maximaliser l'utilisation des données gouvernementales au profit des parties prenantes ;
2. d'améliorer la conception de politiques au sein du gouvernement ;
3. de soutenir les recherches menées par divers organismes ou agences de recherche gouvernementaux ;
4. de détecter des fraudes potentielles ;
5. d'établir le profil des contribuables de manière non intrusive.

En outre, si certains échanges comme ceux qui ont lieu entre ICEGATE et DGFT & DGCIS sont structurés et bien établis, la plupart des autres échanges consistent en des demandes

ponctuelles, ce qui met en évidence le besoin de structurer ce processus de gestion et de communication de données et de lui apporter plus de rigueur.

Tout ce qui précède souligne l'impérative nécessité pour la CBEC de formuler une politique de partage des données ainsi qu'un protocole d'échange de données avec les entités externes en Inde. Avec le temps, il pourrait également être envisageable de mettre en place un protocole d'échange de données similaire avec des entités externes situées en dehors de l'Inde.

Parmi les aspects importants à traiter dans la politique de partage des données figurent :

- la portée et le champ d'application ;
- la catégorisation des données ;
- la catégorisation des utilisateurs ;
- la catégorisation des demandes et modalités de partage des données ;
- le financement du partage de données ;
- le stockage et la conservation des données ;
- la clause de réciprocité ;
- la clause de sauvegarde.

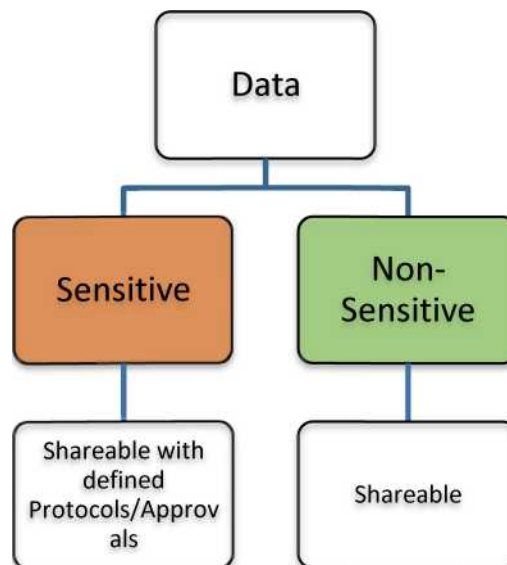
2.3 Portée et champ d'application

Ce document définit la politique régissant les échanges d'informations entre la CBEC et les agences externes située en Inde.

Sous réserve de l'approbation par l'autorité compétente d'un contenu de données dûment identifié, l'échange de données avec des agences externes situées en dehors de l'Inde est régi par un document autonome et distinct : le ***Protocole de la CBEC en matière de connectivité informatique avec des entités étrangères.***

Si l'applicabilité de cette politique se concentre principalement sur la Direction des systèmes (CBEC) puisque la plupart des données sont échangées par voie électronique, la question de son applicabilité aux bureaux de terrain du CBEC et à d'autres directions doit également être posée, en particulier au vu des préoccupations des associations professionnelles concernant la disponibilité de données commerciales sensibles dans le domaine public.

3. La catégorisation des données



Les données disponibles auprès de la CBEC sont classées de sorte à pouvoir être partagées en fonction de différents critères : sensibilité, granularité, aspect critique et propriété/origine des données. En fonction de la catégorisation des données prescrites dans la NDSAP, les données sont ensuite classées comme « partageables » ou « non partageables ». Comme l'indique le schéma ci-dessus, les éléments de données de la CBEC ont été classés comme « sensibles » et « non sensibles ». La communication de données relevant de la catégorie « sensible » se fait habituellement au cas par cas suite à une demande autorisée précise et s'appuie sur un Accord de non-divulgence entre le demandeur et la CBEC. Dans le cas de demandes de données régulières/périodiques, le demandeur doit conclure un Protocole d'accord (Annexe G) et un Accord de non-divulgence avec la CBEC.

3.1 Données sensibles

Les catégories de données suivantes doivent être traitées comme sensibles :

- 3.1.1. Informations personnelles sensibles (IPS) et informations identifiables personnellement (IIP) :** Conformément à la Loi de 2000 sur les technologies de l'information (révisée en 2008), les Informations personnelles sensibles (IPS) et les informations identifiables personnellement (IIP) sont très sensibles. Toutes les données relatives à une entité individuelle doivent donc être classées comme sensibles.
- 3.1.2. Informations commercialement sensibles ayant des implications financières pour un contribuable :** Les données qui pourraient avoir un impact économique sur une entité soumise à l'impôt si elles venaient à être dévoilées (détails de facturation, informations relatives aux tarifs, coordonnées des fournisseurs, etc.) doivent être classées comme sensibles.
- 3.1.3. Données générées grâce aux fonctions de lutte contre la fraude de la CBEC :** Les données générées dans le cadre de l'analyse interne au moyen des outils et techniques internes de profilage de la CBEC dans le cadre des fonctions de lutte contre la fraude, de l'analyse des risques, des enquêtes et des collectes de renseignements, etc., doivent être considérées comme sensibles. Cela inclut les données contenues dans le DRIPS, les données relatives aux infractions et les détails des interceptions du RMS.
- 3.1.4. Données relatives à la configuration/aux technologies des systèmes informatiques de la CBEC**
- 3.1.5. Données granulaires relatives aux journaux d'accès ou d'activité d'une personne dans le système et autres données médicolégaux disponibles dans les systèmes informatiques de la CBEC**
- 3.1.6. Les données fournies à la CBEC par une autre organisation gouvernementale en Inde ou tout autre organisme par le biais d'un dispositif en vigueur (comme les données IEC du DGFT) ou avec qui la CBEC a signé un Protocole d'accord ou un Accord de non-divulgence relèveront de la catégorie des données sensibles.**
- 3.1.7. Données transactionnelles granulaires de parties tierces :** Les données transactionnelles granulaires de tiers contenues dans les documents individuels d'importation/exportation, les restitutions, les paiements, etc., doivent normalement être traitées comme des données sensibles, compte tenu de leur sensibilité commerciale. Si la granularité des informations contenues dans de

telles données ne permet pas nécessairement d'identifier directement une entité commerciale, de telles données pourraient toutefois être liées à la fabrication de marchandises précises dans un domaine particulier ou aux tendances d'évaluation d'un produit de base importé depuis un pays d'origine particulier. Du point de vue du profilage des importations au niveau des produits de base et de la production nationale, les informations qu'elles contiennent seraient également considérées comme sensibles.

3.1.8.

Les informations/données reçues en vertu d'un traité ou d'accords internationaux sont également classées comme des données sensibles.

3.2 Données non sensibles

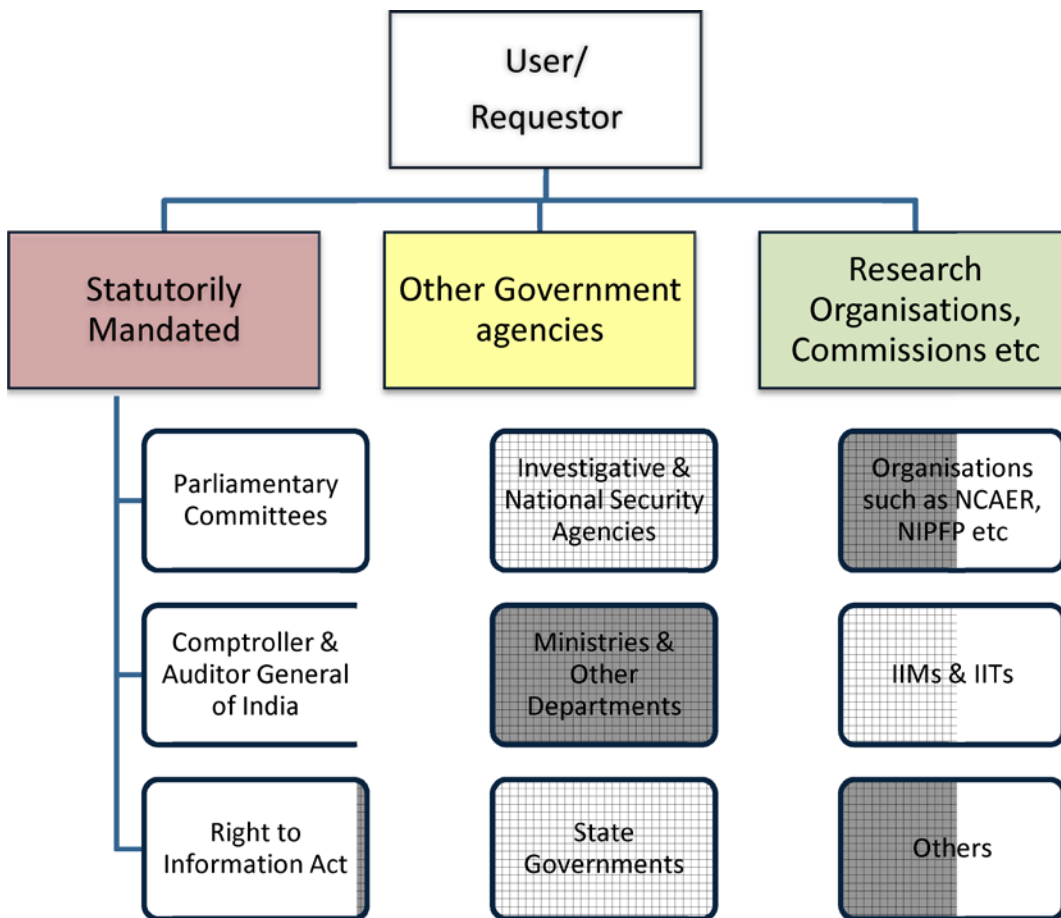
Les données hautement résumées ou agrégées qui ont été générées en combinant des informations sur les personnes physiques et morales sont considérées non sensibles. Les données que les statuts, d'autres lois en vigueur et/ou des décisions politiques de l'Administration imposent d'afficher publiquement ou sur le ou les sites de la CBEC sont traitées comme faisant partie de cette catégorie.

Les données placées sur le site Web de la CBEC conformément à la loi sur le droit à l'information et les accords/pratiques de longue date, comme le Rapport quotidien des échanges (*Daily Trade Report, DTR*), doivent également relever de cette catégorie.

Si elle le juge utile, la CBEC peut décider de diffuser publiquement toutes les données qu'elle estime nécessaires dans l'intérêt de la transparence ou du bien public.

Les modalités de partage de ces données non sensibles pour lesquelles la CBEC reçoit des demandes sont régies par le processus prescrit pour la réception de demandes ponctuelles de données. Une entité faisant une demande de données non sensibles serait donc tenue de se conformer au modèle prescrit (Annexe E) et d'indiquer le nom de la personne dûment autorisée à recevoir ces données. Une fois la demande traitée, la CBEC transmet les données à l'adresse électronique officielle du demandeur.

4. La catégorisation des utilisateurs



Le diagramme ci-dessus illustre la catégorisation des demandeurs de données provenant de la CBEC. Dans l'ensemble, il existe trois catégories :

4.1 Mandaté par Statut

Cette catégorie comprend les agences ou organismes habilités par Statut à demander des données, comme les comités parlementaires, le Contrôleur et Vérificateur général de l'Inde et les bureaux qui en relèvent (comme le CERA) et des requérants dans le cadre du champ d'application de la loi sur le droit à l'information. Les demandes relevant de cette catégorie reçoivent la plus haute priorité et sont traitées en tant que telles. La communication de données relevant de la catégorie « sensible » se fait habituellement au cas par cas suite à une demande autorisée précise et s'appuie sur un Accord de non-divulgence entre le demandeur et la CBEC. Dans le cas de demandes de données régulières/périodiques, le demandeur doit conclure un Protocole d'accord (Annexe G) et un Accord de non-divulgence avec la CBEC.

4.2 Autres agences gouvernementales

Cette catégorie couvre d'autres agences ou organismes gouvernementaux tels que les

organismes de sécurité nationale, les organismes d'investigation hors CBEC, d'autres ministères et départements, les ministères État, etc. La communication de données relevant de la catégorie « sensible » se fait habituellement au cas par cas suite à une demande autorisée précise et s'appuie sur un Accord de non-divulgence entre le demandeur et la CBEC. Dans le cas de demandes de données régulières/périodiques, le demandeur doit conclure un Protocole d'accord (Annexe G) et un Accord de non-divulgence avec la CBEC.

4.3 Organismes de recherche, commissions, etc.

Cette catégorie couvre les demandes provenant d'institutions universitaires et de recherche telles que le Conseil national de la recherche économique appliquée (NCAER), l'Institut national des finances et des politiques publiques (NIPFP), les Instituts indiens de recherche sur la gestion (IIM), les Instituts indiens de technologie (IIT), etc. Elle couvre les demandes émanant de commissions ou de groupes de travail spécialement mis en place, etc. D'ordinaire, les demandes de ces organisations sont uniquement acceptées dans le cas de données non sensibles. Dans l'éventualité d'une commission ou d'un groupe de travail spécialement mis en place recherchant des données sensibles, la CBEC examinera les demandes au cas par cas et décidera si ces données peuvent être fournies. Si la CBEC décide de fournir ces données, toutes les conditions liées au partage des données sensibles telles qu'un Protocole d'accord et un Accord de non-divulgence sont applicables. En outre, ces demandes ne seraient examinées qu'après le traitement des demandes en attente dans la catégorie prioritaire.

5. Catégorisation des demandes et modalités de partage des données

La modalité de partage des données dépend de la catégorisation des données et de leur volume. Les demandes de données sont classées dans deux catégories :

1. demandes ponctuelles ;
2. échanges périodiques structurés de données identifiées.

5.1 Demandes ponctuelles

Dans cette catégorie, le partage des données répond à des demandes spécifiques. Cette catégorie couvre les demandes de quantités de données limitées pour des entités spécifiques et elle est liée à une exigence, une investigation ou une enquête organisationnelle. Les demandes ne seront acceptées que si elles suivent le modèle prescrit (Annexe E). Ce modèle sera disponible sur le site de la CBEC : www.cbec.gov.in.

Si les données se rapportent à une investigation/enquête menée par un organisme de lutte contre la fraude, la CBEC peut envisager de fournir ces données à une personne dûment autorisée par l'organisme en question.

Lorsqu'une demande de ce type est soumise par la Direction des systèmes, les données ne peuvent être fournies qu'avec l'approbation du Directeur général (Systèmes).

Dans ce cas, les données doivent normalement être envoyées à l'adresse électronique officielle du demandeur en réponse au modèle de demande de données (Annexe E) reçu par courrier ou, de préférence, en version papier. S'il est constaté que le courriel ainsi reçu ne provient pas d'un vrai domaine ou s'il est diagnostiqué comme malveillant, la CBEC se réserve le droit de prendre les mesures requises, y compris une expertise judiciaire informatique réalisée par des auditeurs tiers ou un recours juridique, le cas échéant. Si un acte de malveillance est constaté, la CBEC peut décider, à sa discrétion, de ne plus fournir de données à ladite entité

5.2 Échanges structurés de données identifiées

Cette catégorie se rapporte aux données devant être échangées à une fréquence définie dans des formats structurés convenus et comprend le partage de données en masse.

Les organisations qui demandent des données relevant de cette catégorie sont tenues de mettre en œuvre un Protocole d'accord et un Accord de non-divulgence formels qui gouverneront ce partage de données. Ils seront en outre tenus de nommer un officier de liaison et un officier de

liaison suppléant tenant lieu de personnes de contact agréées en charge de la transmission de données et des communications en lien avec cette dernière.

Les données de cette catégorie doivent normalement être échangées par le biais d'un mécanisme électronique sécurisé. En temps voulu, la CBEC envisage de sécuriser ce type d'échange au moyen de signatures numériques tant au niveau personnel que du serveur.

6. Financement du partage de données

La CBEC se réserve le droit de percevoir une somme nominale destinée à couvrir les coûts de production des données dans des formats personnalisés spécifiques. Ces redevances seront déterminées après la procédure d'approbation de l'autorité compétente et conformément aux politiques gouvernementales applicables. Actuellement, la CBEC fournit les données gratuitement, indépendamment de leur complexité et de leur taille.

7. Stockage et conservation des données

Les données sensibles fournies par la CBEC en vertu de la présente politique doivent être stockées dans un système sécurisé dont l'accès est exclusivement réservé au personnel autorisé. Les données ne doivent être conservées que tant qu'elles n'ont pas été utilisées aux fins pour lesquelles elles ont été recueillies. Elles doivent ensuite être effacées en toute sécurité. L'organisation ayant demandé les données sera tenue entièrement responsable de leur divulgation.

8. Clause de réciprocité

Les agences gouvernementales, les organismes de recherche, etc. soumettant une demande d'informations/de données auprès de la CBEC seront tenus de partager les données qu'ils possèdent et que leur demande la CBEC si une telle demande était formulée. La clause de réciprocité fait partie du Protocole d'accord/de l'Accord que la CBEC conclut avec ces organismes/agences pour le partage des données avec ces derniers.

9. Clause de sauvegarde

Toute organisation/entité recevant des données de la CBEC en vertu de la présente politique assume toute responsabilité juridique découlant d'une quelconque action précipitée prise par ladite organisation/entité sur la base desdites données.

Le destinataire des données doit veiller à ce que les données contenant des informations qualifiées de confidentielles par la CBEC, ou mutuellement reconnues comme confidentielles par la CBEC et le destinataire, demeurent confidentielles et ne soient pas divulguées ou transmises à

des personnes non autorisées ni utilisées à des fins autres que celles prévues par les parties. Lorsqu'elle est autorisée, la transmission ultérieure de ces informations confidentielles est soumise au même degré de confidentialité.

Les données partagées ne seront pas considérées comme contenant des informations confidentielles, dans la mesure où de telles informations appartiennent au domaine public. La CBEC et le destinataire peuvent convenir d'utiliser une forme spécifique de protection des données, comme une méthode de chiffrement, dans la mesure autorisée par la loi.

10. Annexe A : Échange actuel de données avec des agences externes

s N°	Type de transfert	Application source	Application cible (interne)/ agence (externe)	Scripts ou directement via l'application/ la base de données	Type de données	Fréquence	Mode de transmission	Mode de transfert (Décharge/ courriel/SFTP/ CD)
1	Presque en temps réel	ICES	EICI	Scripts	Décharge des répertoires sélectionnés	Une fois par jour à 6 h 30	Automatisé	SFTP public
2	Presque en temps réel	ICES	SEZ en ligne	Scripts	Décharge des répertoires sélectionnés	Sur demande	ICEGATE	SFTP public
3	Périodique	ICES	CAG	Scripts	Décharge des imports/ exports ICES – Par exercice financier	Sur demande	SI/ICES	Par CD
4	Presque en temps réel	ACES	EASIEST (NSDL)	Direct à travers l'application	Données d'enregistrement de l'évalué	Deux fois par jour à 8 h et 20 h	Automatisé	SFTP public

s N°	Type de transfert	Application source	Application cible (interne)/ agence (externe)	Scripts ou directement via l'application/ la base de données	Type de données	Fréquence	Mode de transmission	Mode de transfert (Décharge/ courriel/SFTP/ CD)
5	Presque en temps réel	EASIEST (NSDL)	ACES	Direct à travers l'application	Données de paiement électronique	Deux fois par jour à 7 h et 19 h	Automatisé	SFTP public
6	Temps réel	ICEGATE	Partenaires institutionnels	Direct à travers l'application	Avec les banques pour les données de documents officiels, Messages de dépositaire, avec DGFT	Temps réel	Automatisé	SFTP public
7	Presque en temps réel	EASIEST (NSDL)	EDW	Direct à travers l'application	Données de paiement électronique	Deux fois par jour à 7 h et 19 h	Automatisé	SFTP public
8	Ponctuel	RBI	ICES/ICEGATE	Scripts	Décharge de code AD	Ponctuel, fournie par RBI pour chargement dans ICES	RBI (Manuel)	Par courriel

s N°	Type de transfert	Application source	Application cible (interne)/ agence (externe)	Scripts ou directement via l'application/ la base de données	Type de données	Fréquence	Mode de transmission	Mode de transfert (Décharge/ courriel/SFTP/ CD)
9	Ponctuel	CBDT	CBEC	Scripts	Données, déclarations et paiements PAN	Sur demande	CBDT (Manuel)	SFTP public
10	Ponctuel	CBEC	MCA	Scripts	Données d'enregistrement et restitutions de l'entreprise	Sur demande	MCA (Manuel)	SFTP public
11	Périodique	DGFT	ICEGATE	Direct à travers l'application	Détails de la licence, IEC	Base horaire par ICEGATE	Automatisé	SFTP public
12	Ponctuel	ICEGATE	DGCIS	Direct à travers l'application	Détails SB et BE quotidiens après OOC et LEO	Une fois par jour par ICEGATE	Automatisé	SFTP public
13	Temps réel	ICEGATE	DGFT	Direct à travers l'application	Détails de la facture d'expédition de l'exportateur	ICEGATE – à vérifier	Automatisé	SFTP public

s N°	Type de transfert	Application source	Application cible (interne)/ agence (externe)	Scripts ou directement via l'application/ la base de données	Type de données	Fréquence	Mode de transmission	Mode de transfert (Décharge/ courriel/SFTP/ CD)
14	Périodique	EDW	DEA		Détails d'importation de l'or	Hebdomadaire/ Mensuelle		Courriel
15	Périodique	EDW	Ministère du Pétrole		Importations personnalisées ; niveau transactionnel pour le gaz naturel liquéfié (GNL)	2 à 3 mois		Courriel
	Périodique	EDW	Direction générale de la lutte antidumping (ministère du Commerce)		Importations personnalisées ; niveau transactionnel	Mensuelle		Courriel

Note : L'équipe EDW a ponctuellement fourni des données avec l'approbation de la DG (Systèmes) à des agences externes tels que le Contrôleur et Vérificateur général de l'Inde, le ministère des Statistiques et de la mise en œuvre des programmes, le Conseil national de la recherche économique appliquée, l'Institut national des finances et des politiques publiques, les services compétents en matière de TVA du Gujarat et du

Pendjab, le Conseil du caoutchouc d'Inde, la Commission Shah, la Commission des réformes administratives fiscales, etc.

11. Annexe B : Échange actuel de données avec des agences internes

S N°	Type de transfert	Application source	Application cible (interne)/agence (externe)	Scripts ou directement via l'application/la base de données	Type de données	Fréquence	Mode de transmission	Mode de transfert (Décharge/courriel/SFTP/CD)
1	Presque en temps réel	ICES	DRI	Scripts	Décharge d'export Oracle pour 1. À l'envoi de BE et SB 2. Fin de la journée après OOC et LEO 3. Fin de la journée données IGM 4. Décharges mensuelles de répertoires pour 14 répertoires	1. À l'envoi, toutes les 2 h 2. Données EOD – Une fois par jour, 3/4 h du matin 3. Données EOD – Une fois par jour, 4 h du matin 4. Mensuelle, tous les 1 ^{ers} du mois à 7 h	Automatisé	DRI SFTP

Politique de partage des données V 0.1 Administration centrale des douanes et accises

S N°	Type de transfert	Application source	Application cible (interne)/agence (externe)	Scripts ou directement via l'application/la base de données	Type de données	Fréquence	Mode de transmission	Mode de transfert (Décharge/courriel/SFTP/CD)
2	Presque en temps réel	ICES	ACES	Scripts	Données IEC	Tous les jours à 6 h 30	Automatisé	SFTP
3	Presque en temps réel	ICES	Calculatrice de droit de douane	Scripts	Décharge des répertoires sélectionnés	Tous les jours à 6 h	Automatisé	SFTP public
4	Presque en temps réel	ICES	Site Web ICEGATE	Scripts	Données sur les recettes quotidiennes (liste quotidienne)	Une fois par jour à 7 h	Automatisé	SFTP/Site Web
5	Presque en temps réel	ACES	ICES	Scripts	Données de remboursement ST	Chaque jour à 0 h 30	Automatisé	SFTP
6	Périodique	ACES	EDE	Directement	Base de données DR pour les données différentielles	Une fois par quinzaine	Automatisé	Base de données
7	Périodique	ICES	EDE	Directement	Base de données DR ICES pour les données différentielles	Tous les jours en matinée	Automatisé	Base de données

Politique de partage des données V 0.1 Administration centrale des douanes et accises

S N°	Type de transfert	Application source	Application cible (interne)/agence (externe)	Scripts ou directement via l'application/la base de données	Type de données	Fréquence	Mode de transmission	Mode de transfert (Décharge/courriel/SFTP/CD)
8	Périodique	ICES	DRI, CBEC	Scripts	Rapport oignon, blé et riz	Hebdomadaire – Tous les lundis	SI (Manuel)	Par courriel
9	Périodique	ICES	DRI, CBEC	Scripts	Rapport mensuel des revenus – Relatif au site	Mensuelle, tous les 1 ^{ers} du mois	SI (Manuel)	Par courriel
10	Périodique	ICES	ICEGATE	Scripts	Dépôt total BE et SB – relatif au site	Tous les jours à 8 h	Automatisé	Par courriel
11	Périodique	EDE	TRU		Détails d'importation de l'or et de l'argent, Données relatives aux produits de base Pol/non-Pol	Mensuelle		Par courriel
12	Périodique	EDE	Président, Bureau de la CBEC		Rapports des recettes de l'accise centrale	Mensuelle		Par courriel
13	Périodique	EDE	Commissaire (douanes et promotion des		Détails d'importation en vertu de divers accords de	Trimestrielle		Par courriel

Politique de partage des données V 0.1 Administration centrale des douanes et accises

S N°	Type de transfert	Application source	Application cible (interne)/agence (externe)	Scripts ou directement via l'application/la base de données	Type de données	Fréquence	Mode de transmission	Mode de transfert (Décharge/courriel/SFTP/CD)
			exportations)		libre-échange (ALE)			

12. Annexe C : ISO 27001/27002

Domaine 13 de la norme ISO/IEC 27001 : 2013 et 27002 (instructions de mise en œuvre)

13 Sécurité des communications

13.1 Gestion de la sécurité réseau

13.2 Transfert d'informations

Objectif : Maintenir la sécurité des informations transférées au sein d'une organisation et avec toute entité externe.
--

13.2.1 Politiques et procédures des transferts d'informations

Contrôle

Les politiques, procédures et contrôles formels de transfert doivent être mise en place pour protéger le transfert des informations à travers par tout moyen de communication.

Guide de mise en œuvre

Les procédures et le contrôle à effectuer lorsque des moyens de communication sont utilisés pour transférer les informations doivent tenir compte des éléments suivants :

- a) les procédures de protection des informations transmises contre l'interception, la copie, la modification, les erreurs de routage et la destruction ;
- b) les procédures de détection des logiciels malveillants susceptibles d'être transmis par voie de communication électronique et la protection contre ces derniers (cf. 12.2.11) ;
- c) les procédures de protection des informations électroniques sensibles transmises en pièces jointes ;
- d) les politiques ou directives décrivant l'utilisation acceptable des moyens de communication (cf. 8.1.3) ;
- e) la responsabilité du personnel, de la partie externe et des autres utilisateurs de ne pas compromettre l'organisation, en pratiquant par exemple la diffamation, le harcèlement, l'usurpation d'identité, la transmission de chaînes de lettres, les achats non autorisés, etc. ;
- f) l'utilisation de techniques cryptographiques, notamment pour protéger la confidentialité, l'intégrité et l'authenticité des informations (cf. clause 10) ;
- g) les directives de conservation et d'élimination de toute correspondance d'affaires, y compris les messages, conformément à la législation et à la réglementation nationales et locales concernées ;
- h) les contrôles et restrictions associés à l'utilisation de moyens de communication, comme le transfert automatique de courriels à des adresses de messagerie externes ;
- i) conseiller au personnel de prendre les précautions nécessaires pour ne pas révéler d'informations confidentielles ;
- j) ne pas laisser de messages contenant des informations confidentielles sur des répondeurs, puisque ces messages peuvent être écoutés par des personnes non autorisées, stockés sur des systèmes communaux ou sur une mauvaise boîte vocale après avoir composé un numéro erroné ;
- k) mettre le personnel au fait des problèmes liés à l'utilisation d'appareils ou de services de télécopie, à savoir :
 - 1) l'accès non autorisé à des messageries intégrées pour récupérer des messages ;

- 2) la programmation délibérée ou accidentelle d'appareils afin d'envoyer un message à des numéros précis,
- 3) l'envoi de documents et de messages à un mauvais numéro après avoir mal composé le numéro ou utilisé un mauvais numéro enregistré.

Il convient par ailleurs de rappeler au personnel qu'il n'est pas autorisé à tenir une conversation confidentielle dans des lieux publics, des bureaux et des lieux de réunion ouverts, ni par le biais de canaux de communication non sécurisés.

Les services de transfert d'informations doivent se conformer aux exigences juridiques en la matière (cf. 18.1).

Informations complémentaires

Le transfert d'informations peut passer par de nombreux moyens de communication, dont le courrier électronique, la télécopie, la voix et la vidéo.

Le transfert de logiciels peut passer par de nombreux canaux, dont le téléchargement en ligne et l'acquisition auprès de fournisseurs vendant des produits disponibles sur le marché.

Il convient de tenir compte des implications juridiques, commerciales et en matière de sécurité associées à l'échange électronique de données, au commerce électronique et aux communications électroniques, mais également des exigences en matière de contrôles.

13.2.2 Accords sur le transfert d'informations

Contrôle

Ces Accords doivent aborder le transfert sécurisé d'informations commerciales entre l'organisation et les parties externes.

Guide de mise en œuvre

Les Accords sur le transfert d'informations doivent contenir les éléments suivants :

- a) les responsabilités en matière de gestion du contrôle et de notification de la transmission, de l'expédition et de la réception des informations ;
- b) les procédures visant à assurer la traçabilité et la non-répudiation ;
- c) les normes techniques minimales pour la constitution des paquets et la transmission;
- d) les conventions de séquestre ;
- e) les normes d'identification du courrier ;
- f) les responsabilités et obligations en cas d'incidents liés à la sécurité des informations, comme une perte de données ;
- g) l'utilisation d'un système d'étiquetage convenu pour les informations sensibles ou critiques garantissant la compréhension immédiate de la signification des étiquettes et la protection des renseignements (cf. 8.21) ;
- h) les normes techniques d'enregistrement et de lecture des informations et des logiciels ;
- i) tous les contrôles spéciaux nécessaires à la protection des éléments sensibles, comme la cryptographie (cf. clause 10) ;
- j) le maintien de la chaîne de surveillance des informations pendant le transit ;
- k) les niveaux de contrôle d'accès acceptables.

Des politiques, procédures et normes doivent être établies et maintenues afin de protéger les informations et les supports physiques pendant leur transit (cf. 8.3.3) et doivent figurer dans ces accords de transfert.

Le contenu de tout accord en matière de sécurité des informations doit refléter la sensibilité des informations commerciales concernées.

Informations complémentaires

Les accords peuvent être électroniques ou manuels et prendre la forme de contrats formels. Les mécanismes spécifiques utilisés pour le transfert d'informations confidentielles doivent être les mêmes pour toutes les organisations et tous les types d'accords.

13.2.3 Messagerie électronique

Contrôle

Les informations transmises par messagerie électronique doivent être protégées de manière appropriée.

Guide de mise en œuvre

Les considérations relatives à la sécurité des informations transmises par messagerie électronique doivent inclure les éléments suivants :

- a) la protection contre les messages provenant d'un accès non autorisé et la modification ou le refus de services en rapport avec le système de classification adopté par l'organisation ;
- b) garantir que le message porte la bonne adresse et en assurer le transport correct ;
- c) la fiabilité et la disponibilité des services ;
- d) les considérations juridiques, notamment les exigences en matière de signatures électroniques ;
- e) l'obtention d'une autorisation préalable à l'utilisation de services publics externes comme la messagerie instantanée, les réseaux sociaux ou le partage de fichiers ;
- f) le renforcement des niveaux d'authentification permettant de contrôler l'accès à des réseaux publics.

Informations complémentaires

De nombreux types de messageries électroniques jouent un rôle dans les communications commerciales, comme le courrier électronique, l'échange de données électroniques et les réseaux sociaux.

13.2.4 Accords de confidentialité ou de non-divulgaration

Contrôle

Les accords de confidentialité ou de non-divulgaration doivent assurer l'exigence de protection des informations confidentielles en utilisant des conditions juridiquement contraignantes. Les accords de confidentialité ou de non-divulgaration sont applicables aux parties externes ou aux employés de l'organisation. La sélection ou l'ajout d'éléments doit tenir compte du type de l'autre partie et de l'autorisation dont celle-ci dispose pour accéder à des informations confidentielles et les traiter. Afin d'identifier les exigences des accords de confidentialité ou de non-divulgaration, les éléments suivants doivent être pris en considération :

- a) la définition des informations à protéger (ex. : informations confidentielles) ;
- b) la durée prévue d'un accord, même dans les cas où il est possible que la confidentialité doive être maintenue indéfiniment ;
- c) les actions requises lors de la résiliation d'un accord ;
- d) les responsabilités et les mesures prises par les signataires pour éviter la divulgation non autorisée des informations ;
- e) la propriété de l'information, les secrets d'affaires, la propriété intellectuelle et leur lien avec la protection des informations confidentielles ;
- f) l'utilisation autorisée des informations confidentielles et les droits du signataire à utiliser ces informations ;
- g) le droit à vérifier et contrôler les activités impliquant des informations confidentielles ;
- h) le processus de notification et de remise de rapports concernant les divulgations non

autorisées ou les fuites d'informations confidentielles ;

- i) les conditions de restitution et de destruction des informations lors de la résiliation de l'accord ;
- j) les mesures à mettre en œuvre en cas de violation de l'accord.

Au vu des besoins des organisations en matière de sécurité des informations, il pourrait s'avérer nécessaire d'inclure d'autres éléments dans un Accord de confidentialité ou de non-divulgence.

L'Accord de confidentialité et de non-divulgence doit se conformer à toutes les lois et réglementations applicables dans la juridiction à laquelle elles s'appliquent (cf. 18.1).

Les exigences des accords de non-divulgence et de confidentialité doivent être examinées périodiquement et quand surviennent des changements susceptibles d'influencer ces exigences.

Informations complémentaires

Les accords de confidentialité et de non-divulgence protègent les informations organisationnelles et informent les signataires qu'ils doivent protéger, utiliser et divulguer les informations d'une manière responsable et dans la limite de ce qui a été autorisé.

Il peut s'avérer nécessaire pour une organisation de recourir à différentes formes d'accords de confidentialité ou de non-divulgence en fonction des circonstances.

13. Annexe D : Protocoles de connectivité informatique

Mise en place de l'échange de données

Le tableau ci-dessous expose les exigences prévues pour l'échange de données électroniques avec le CBEC :

S. N°	Paramètre	Modalité
1	Connectivité	Aucune connexion directe aux serveurs de production de la CBEC ne sera accordée aux partenaires internationaux. L'échange de messages se fera en plaçant des fichiers dans des répertoires désignés (en distinguant les répertoires Entrée et Sortie) et en les assortissant d'autorisations spécifiques.
2	Connectivité réseau	Le mode par défaut pour l'établissement d'une communication doit être une connexion VPN SSL de site à site.
3	Adresse IP statique	Seuls les périphériques disposant d'une adresse IP/MAC statique et déclarée recevront un droit d'accès
4	Port réseau pour les données entrantes	La communication sera uniquement autorisée sur le port spécifié.
5	Authentification	Authentification par signature numérique au moyen de certificats numériques de classe III TACACS/CHAP
6	Chiffrement	ISAKMP (<i>Internet Security Association and Key Management Protocol</i>) ; AES ; AS2 ; SHA
7	Type de fichier	Formats de fichiers texte et XML
8	Taille maximale des fichiers	Un seul fichier sera accepté pour chaque transaction. La taille maximale autorisée pour ce fichier sera de 10 Ko
9	Fonction de hachage	Le hachage sera mis en œuvre pour vérifier l'intégrité des fichiers échangés – SHA.
10	Accord de non-divulgaration ou d'utilisation	Une agence se connectant aux systèmes informatiques de la CBEC met en application un accord mutuellement convenu de non-divulgaration ou d'utilisation acceptable

S. N°	Paramètre	Modalité
	acceptable	des données de la CBEC, stockage et archivage inclus.
11	Journaux d'audit	Des journaux d'audit seront créés pour chaque transaction et activité de l'utilisateur. Ils peuvent faire l'objet d'audits menés par des tiers et mandatés par la CBEC.
12	Autre	Les outils ne prenant pas en charge l'enregistrement ou l'établissement d'historiques traçables (incluant mais ne se limitant pas à Winscp) ne doivent être utilisés par aucune des deux parties.

Serveur de communication : La CBEC créera des répertoires Entrée et Sortie distincts sur son serveur de communication. Les fichiers à envoyer au partenaire international seront placés dans le répertoire de sortie par la CBEC. Inversement, les fichiers à recevoir de la part du partenaire international seront placés dans le dossier d'entrée par le partenaire international.

Purge/Archivage des données : Lorsqu'un fichier sera récupéré dans le répertoire d'entrée par les systèmes informatiques de la CBEC, il sera purgé dans un délai convenu n'excédant pas 7 jours.

Canal de communication : Il importe que les deux parties maintiennent des lignes de communication claires ; pour ce faire, elles doivent s'échanger les coordonnées du ou des fonctionnaire(s) responsable(s) de l'échange des données, ainsi que des coordonnées d'urgence. Les cas d'arrêt planifiés et non planifiés seront communiqués à l'autre partie.

Protocole de réaction à un incident : Les deux parties se notifieront mutuellement en cas d'intrusion, d'attaque ou d'utilisation abusive des données. En cas d'atteinte à la sécurité, les deux parties coordonnent leurs activités de réaction à l'incident.

Gestion du changement

Si la politique et les procédures de sécurité informatique de la CBEC venaient à être actualisées, la mise à jour correspondante du protocole d'échange des données devra être notifiée au partenaire international. Le protocole actualisé devra ensuite être traité comme une norme obligatoire dans l'échange de données entre la CBEC et le partenaire international.

Interruption de l'échange de données

- **Interruption prévue :** En cas d'interruption justifiée de l'échange de données, la partie prenant l'initiative notifiera l'autre partie par écrit et recevra un avis de réception en retour.

La notification devra décrire la ou les raisons de la déconnexion et fournir le calendrier de la déconnexion.

- **Interruption d'urgence** : Si une partie ou les deux parties détecte(nt) une attaque ou tout autre risque exploitant ou menaçant les systèmes informatiques ou les données, l'échange de données peut être interrompu sans nécessité de préavis écrit à l'autre partie. Si une telle action est justifiée, elle doit toutefois être notifiée à l'autre partie dans les meilleurs délais après cette date.

Toutes les exigences ci-dessus peuvent être modifiées moyennant l'accord du Responsable de la sécurité des systèmes d'information de la CBEC (*Chief Information Security Officer, CISO*).

14. Annexe E : Modèle de demande

MODÈLE DE DEMANDE DE DONNÉES PAR DES ORGANISMES EXTERNES EN INDE		
S. N°	Détails	Description
1	Nom de l'organisation demandeuse	
2	Mandat pour la recherche de données (Statutaire/Protocole d'accord/Accord, etc.)	
3	Nom du demandeur – Interlocuteur unique	
4	Désignation du demandeur	
5	Courriel officiel du demandeur	
6	Numéro de contact direct du demandeur	
7	Adresse officielle du demandeur	
8	Données demandées – Douane/accise centrale/services fiscaux	
9	Brève description de l'objectif	
10	Éléments de données demandés (Source de l'élément, le cas échéant. Par exemple : enregistrement/restitution/paiements, etc.)	
11	Position tarifaire des douanes/accises centrales (le cas échéant) *	
12	Période pour laquelle les données sont demandées	
13	Format du rapport, le cas échéant	
14	Exigences complémentaires, le cas échéant	

*Si la position tarifaire n'est pas donnée, la communication des données connaîtra un retard

ENGAGEMENT (facultatif si un Protocole d'accord valable a été conclu avec la CBEC)

Je/Nous _____ (nom de l'organisation) déclare/déclarons par la présente que les données demandées ci-dessus ne sont sollicitées qu'à des fins officielles et je prends/nous prenons l'engagement de veiller à accorder un degré de sécurité et de confidentialité aussi élevé que celui appliqué aux données sécurisées de notre propre organisation. Je prends/Nous prenons également par la présente l'engagement de ne pas partager ultérieurement les données fournies par la CBEC sans en avoir reçu le consentement écrit. Je prends/Nous prenons en outre l'engagement d'assumer toute responsabilité juridique découlant d'une quelconque mesure précipitée prise par mon/notre organisation/entité concernant la base de données transmise par la CBEC.

Je/Nous _____ (nom de l'organisation) prends/prenons en outre l'engagement d'être tenu(s) de partager des données nous appartenant si la CBEC nous en fait la demande.

Signature _____

Prénom _____

Localité _____

Date _____

Pour usage interne à la CBEC

Demande Accusé de réception N° _____

(S.N°/JJmoiAAAA, p. ex. 1/01jan2014)

Date de réception de la demande _____

N° de fichier Direction des systèmes, le cas échéant _____

N° de ticket de la demande (généré par le système), le cas échéant _____

Demande Approuvée par _____

Date d'approbation de la demande _____

Date de clôture de la demande _____

Méthode de transmission (rayer les mentions inutiles) :

- via l'adresse électronique officielle
- par FTP sécurisé
- sur un support physique (avec approbation)
- sur papier

15. Annexe F : Proposition de procédure de partage des données

1. Toutes les demandes de données adressées à la Direction des systèmes doivent suivre la procédure suivante :
 - a. Le responsable de l'agence demandeuse doit écrire à la CBEC et lui fournir les détails de la demande, comme l'objectif de la demande de données, les champs de données requis et la périodicité des données recherchées. Il doit également désigner l'interlocuteur unique de son département, qui interagira avec les responsables concernés de la DG Systèmes et dont il communiquera les coordonnées (adresse, numéro de téléphone, télécopie et adresse électronique officielle sur NIC ou un autre domaine gouvernemental) en vue de toute correspondance ultérieure. L'interlocuteur unique pourra par la suite envoyer par courrier ou par courriel à la Direction des systèmes les demandes de données distinctes ou complémentaires adressées au même bureau.
2. La demande de récupération/analyse des données adressée à la CBEC par des agences externes doit préalablement être approuvée en principe par le gestionnaire du projet (Projet EDW) de la CBEC avant que l'équipe EDE n'examine la faisabilité de la communication des données.
3. La faisabilité de la communication des données demandées doit alors être examinée par l'équipe EDW, qui peut contacter l'interlocuteur unique du bureau pour lui demander des précisions si des éclaircissements s'avèrent nécessaires, avec l'approbation du gestionnaire du projet (Projet EDW) de la CBEC.
4. Si la récupération de données n'est pas faisable, l'agence demandeuse en sera immédiatement informée.
5. Une fois les données récupérées/analysées, elles doivent être partagées avec le gestionnaire du projet (Projet EDW) de la CBEC pour révision.
6. Après la révision et la correction des données, le cas échéant, il est nécessaire d'obtenir l'approbation de l'envoi des données en écrivant à la DG (Systèmes) à travers l'ADG.
7. Les données seront envoyées uniquement à l'adresse électronique officielle de l'interlocuteur unique (de préférence NIC) du bureau qui a envoyé la demande de données.
8. Si les données sont volumineuses, elles seront transmises au fonctionnaire concerné par SFTP (*Secured File Transfer Protocol*). La modalité de ce transfert SFTP sera régie par la

méthodologie exposée à l'Annexe D.

9. En général, l'extraction des données ne se fait pas au moyen d'un support physique (CD, clé USB, etc.). Des exceptions à cette règle peuvent être admises si elles sont préalablement approuvées par la DG (Systèmes).
10. Toutes les réponses aux demandes formulées par l'interlocuteur unique du bureau pour obtenir des données après l'approbation du gestionnaire du projet EDW doivent être transmises au centre d'assistance technique EDW.
11. Si une demande de données émanant d'une agence externe est transmise à un bureau de la CBEC, elle sera ensuite traitée comme une demande interne et la réponse à cette demande sera envoyée au fonctionnaire concerné de la CBEC.
12. À des fins d'archivage, l'équipe EDW doit conserver les journaux de toutes les demandes de données externes, la correspondance et les courriels s'y afférant ainsi que les copies électroniques des données fournies.
13. Il convient de suivre les étapes mentionnées ci-dessus pour toutes les demandes de données reçues de la part des agences externes. Tout écart à ces procédures en cas de circonstances exceptionnelles devra avoir obtenu l'approbation de la DG (Systèmes).

16. Annexe G : Projet de Protocole d'accord

PROTOCOLE D'ACCORD

ENTRE

L'ADMINISTRATION CENTRALE DES DOUANES ET ACCISES, MINISTÈRE DES
FINANCES, GOUVERNEMENT DE L'INDE

ET

POUR

L'ÉCHANGE DE DONNÉES VISANT À RENFORCER LA CONFORMITÉ FISCALE

Ce Protocole d'accord est conclu le _____ du mois de _____

ENTRE

l'Administration centrale des douanes et accises (CBEC), le Service des perceptions, le ministère des Finances, le gouvernement de l'Inde, représenté par **le Directeur général, la Direction des systèmes (DdS), les Douanes et accises centrales**, et/ou la/les personne(s) autorisée(s) par écrit par la CBEC à la représenter à cet égard, ci-après dénommée(s) « CBEC » (expression qui, à moins d'être exclue par ou incompatible avec le contexte, désignera son ou ses successeurs au poste ou ses cessionnaires) ou PREMIÈRE PARTIE.

ET

_____ et/ou la/les personne(s) autorisée(s) par écrit par _____ à la représenter à cet égard, ci-après dénommée _____ (expression qui, à moins d'être exclue par ou incompatible avec le contexte, désignera son ou ses successeurs au poste ou ses cessionnaires) ou SECONDE PARTIE.

Attendu que le besoin d'un mécanisme structuré permettant l'échange régulier de champs de données identifiés entre la CBEC et _____ pour _____ (objet de la signature du Protocole d'accord) a été reconnu, ce Protocole d'accord est exécuté par les parties de la première et de la seconde partie :

Article 1

Objet et portée

1.1 Le « Protocole d'accord » précise les conditions en vertu desquelles les parties échangeront des données.

1.2 Le Protocole d'accord inclut les dispositions énoncées ci-dessous et sera complété par les Annexes, qui feront partie intégrante du présent Protocole d'accord.

1.3 À moins qu'il n'en soit convenu autrement par les parties, l'échange de données doit se faire par voie électronique sécurisée.

Article 2

Définitions

Aux fins du Protocole d'accord, les termes suivants sont définis comme suit :

2.1 Partie émettrice : Première ou seconde partie, le cas échéant, qui fournit des données.

2.2 Partie réceptrice : Première ou seconde part, le cas échéant, à qui des données sont fournies.

2.3 Exercice financier : Un exercice financier est l'année pendant laquelle des recettes sont perçues. Il s'agit une période de douze mois à compter du 1^{er} avril d'une année donnée au 31 mars de l'année suivante.

2.4 Année d'évaluation : Une année d'évaluation désigne une période de douze mois commençant le 1er avril de chaque année et se terminant le 31 mars de l'année succédant immédiatement à l'année précédente.

2.5 Jour ouvrable : Un jour ouvrable est un jour autre qu'un samedi, dimanche ou jour férié officiel dans le pays de la Partie réceptrice.

2.6 Service destiné aux gros contribuables (*Large Taxpayer Unit*, LTU) : Un LTU est un bureau fiscal autonome relevant du Service des perceptions et tenant lieu de guichet unique pour toutes les questions relatives à l'accise centrale, l'impôt sur le revenu, l'impôt sur les sociétés et les taxes sur les services.

Article 3
Validité et conformité

3.1 Le Protocole d'accord est valable pour une période de trois ans et entrera en vigueur à partir du _____ (date). Après l'expiration de sa validité, le Protocole d'accord peut être prolongé par consentement mutuel des deux parties.

3.2 Chaque Partie veillera à ce que les données envoyées ou reçues soient conformes aux formats et fréquences convenus, fournis en Annexe.

Article 4
Utilisation des données échangées dans le cadre d'une procédure juridique

Dans la mesure permise par la législation indienne applicable, les parties conviennent par la présente qu'en cas d'utilisation des données ainsi échangées dans un tribunal dans le cadre d'une procédure civile ou pénale, ces données devront être étayées par des preuves documentaires et d'autres documents statutaires, conformément à la loi sur les douanes, la loi sur l'accise centrale, les lois fiscales relatives aux impôts sur les sociétés prévues par la loi de finances de 1994 et à toute autre loi en vigueur.

Article 5
Modalité d'échange et avis de réception

5.1 Sauf mention contraire, les données doivent être échangées par le biais d'un mécanisme électronique sécurisé.

5.2 Sauf mention contraire, l'avis de réception doit être envoyé par voie électronique.

5.3 La Partie réceptrice veillera à envoyer un avis de réception à la Partie émettrice dans les deux jours ouvrables suivant la réception des données, à moins d'avoir convenu d'un autre délai.

5.4 Les parties émettrice et réceptrice conserveront toutes deux un dossier horodaté des fichiers transmis et reçus.

Article 6
Sécurité des données partagées

6.1 Les parties s'engagent à mettre en œuvre et à maintenir des procédures et des mesures de sécurité visant à assurer la protection des données partagées contre les risques d'accès non autorisé, de modification, de retard, de destruction ou de perte.

6.2 Les procédures et les mesures de sécurité peuvent inclure la vérification de l'origine, la vérification de l'intégrité, la non-répudiation de l'origine et de la réception et la confidentialité des données partagées. S'il y a lieu, des procédures et des mesures de sécurité supplémentaires

peuvent être expressément formulées et mutuellement convenues.

6.3 Si l'utilisation des procédures et des mesures de sécurité entraîne le rejet ou la détection d'une erreur dans les données partagées, le récepteur en informera l'émetteur dans le délai indiqué.

Lorsqu'une donnée rejetée ou erronée est retransmise par l'émetteur, les données doivent indiquer clairement qu'il s'agit d'une retransmission de données corrigées.

Article 7

Confidentialité et sauvegarde

7.1 Les parties doivent veiller à ce que les données contenant des informations qualifiées de confidentielles par l'émetteur, ou mutuellement convenues comme étant confidentielles par les parties, restent confidentielles et ne soient pas divulguées ou transmises à des personnes non autorisées ni utilisées à des fins autres que celles prévues par les parties.

Lorsqu'elle est autorisée, la transmission ultérieure de ces informations confidentielles est soumise au même degré de confidentialité.

7.2 Les données partagées ne seront pas considérées comme contenant des informations confidentielles, dans la mesure où de telles informations appartiennent au domaine public.

7.3 Les parties peuvent convenir d'utiliser une forme spécifique de protection des données, telle qu'une méthode de chiffrement, dans la mesure autorisée par la loi.

7.4 Un dossier complet et chronologique de toutes les données échangées par les parties doit être conservé par chaque Partie dans sa version intégrale et en toute sécurité, conformément aux délais et aux spécifications prescrites par les exigences législatives et, dans tous les cas, pendant la durée du Protocole d'accord.

7.5 Toute organisation/entité recevant des données de la part de la CBEC en vertu de la présente politique assume toute responsabilité juridique découlant d'une quelconque mesure précipitée prise par ladite organisation/entité sur la base desdites données.

Article 8

Clause de réciprocité

8.1 Les agences gouvernementales, les organismes de recherche, etc. soumettant une demande d'informations/de données auprès de la CBEC seront tenus de partager les données qu'ils possèdent et que leur demande la CBEC, si une telle demande était formulée. Cette clause

de réciprocité sera incluse dans le Protocole d'accord/Accord conclu par la CBEC avec lesdits organismes/agences en vue d'un partage de données avec ces derniers.

Article 9

Exigences opérationnelles encadrant l'échange de données

9.1 Les parties s'engagent à mettre en œuvre et à maintenir un environnement opérationnel pour procéder à des échanges de données, conformément aux conditions du présent Protocole d'accord, qui comprend sans s'y limiter les éléments suivants :

a. Équipement opérationnel

Les parties doivent fournir et assurer la maintenance des équipement, logiciels et services nécessaires pour transmettre, recevoir, enregistrer, traiter et stocker les données partagées.

b. Mode de communication :

Sauf indication contraire, le mode de communication par défaut pour les questions opérationnelles liées à l'échange de données est le courriel officiel des personnes autorisées par les parties.

Article 10

Responsabilités des parties

10.1 Responsabilités des parties

Pour faciliter l'échange des données, les Parties sont tenues de :

1. Désigner un ou des agents de liaison qui agiront en qualité d'interlocuteurs pour coordonner l'échange de données ;
2. Accorder la priorité et les ressources nécessaires à l'accomplissement des tâches liées à l'échange de données dans les délais prévus.
3. Établir un mécanisme destiné à résoudre les problèmes de qualité des données, le cas échéant, dans un délai raisonnable.
4. Établir un mécanisme de révision périodique de l'échange des données et de ses résultats.

Article 11

Conditions générales

11.1 Absence de considérations commerciales

Les parties conviennent mutuellement qu'il n'existe aucune considération commerciale vis-à-vis du présent Protocole d'accord.

11.2 Indemnisation

La CBEC et _____ acceptent de s'indemniser mutuellement pour les effets indirects découlant des mesures prises en vertu du présent Protocole d'accord.

11.3 Force majeure (peut être enlevée du fait de l'absence de considérations commerciales)

- i. _____ et la CBEC ne seront pas tenus responsables du non-respect des obligations en cas de force majeure.
- ii. Un obstacle de force majeure renvoie à un événement imprévu se produisant après la signature du présent Protocole d'accord, notamment une grève, un blocus, une guerre, une mobilisation, une révolution ou des émeutes, une catastrophe naturelle, un cas fortuit, un refus de licence par les Autorités de l'État ou du gouvernement central, dans la mesure où un tel événement empêche la Partie contractuelle de remplir ses obligations ou la retarde dans leur exécution.
- iii. Dans l'éventualité où les conditions de force majeure se prolongent pendant plus de 60 jours, toutes les parties devront discuter de l'effet de ces conditions sur le Protocole d'accord et se prononceront sur la marche à suivre.

Il n'est pas possible de poursuivre une Partie de ce Protocole d'accord pour son incapacité à se conformer aux dispositions du Protocole d'accord du fait de circonstances indépendantes de sa volonté.

11.4 Déviations et résolution des différends

Sur tous les aspects qui ne sont pas abordés dans les articles ci-dessus du présent Protocole et dans les cas particuliers de dérogation à ces articles, la décision mutuellement convenue entre _____ et la CBEC sera définitive.

11.5 Résolution des différends

En cas de litige relatif à ou découlant du présent Protocole d'accord, le différend sera réglé à l'amiable par consultation mutuelle. Si une telle résolution n'est pas possible, le différend ou litige non réglé doit être renvoyé à un comité composé du Secrétaire (Perceptions), du Président de la CBEC, _____ et de tout membre coopté par l'autre Partie, dont la décision sera obligatoire pour les deux Parties.

11.6 Clause de sortie

Chacune des parties peut résilier le présent Protocole d'accord en donnant un préavis de trois mois à chaque Partie, conformément aux conditions mutuellement convenues.

Au moment de l'expiration/la résiliation du présent Protocole d'accord, aucune Partie du Protocole d'accord ne sera tenue responsable de quelque façon que ce soit (technique, financière, juridique, etc.) des éventuelles conséquences provoquées sur l'autre Partie par des événements survenus après cette expiration/résiliation.

11.7 Amendement du Protocole d'accord

Aucune vérification ou modification des conditions du présent Protocole d'accord ne sera effectuée autrement que par amendement écrit signé par les deux parties.

EN FOI DE QUOI, les parties ont signé le présent accord en double exemplaire, le jour et l'année indiqués ci-dessous.

AU NOM DE ET POUR LE COMPTE DE
LA CBEC

Signature

Nom :

Désignation :

Date :

Localité :

Signature

Nom :

Désignation :

Date :

Localité :

EN PRÉSENCE DE

Signature

Nom :

Désignation :

Date :

Localité :

EN PRÉSENCE DE

Signature

Nom :

Désignation :

Date :

Localité :

17. Annexe H : Définitions

S. N°	Terme	Définition
1	EDW	Un entrepôt de données d'entreprise (EDW) est un dépôt central d'informations d'entreprise conçu pour les demandes et les analyses plutôt que pour le traitement de transactions au jour le jour. Il contient des données provenant de multiples applications comme des historiques.
2	ISO 27001	La norme ISO 27001 est une norme de sécurité de l'information publiée par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) dans le cadre du sous-comité mixte ISO et IEC, ISO/IEC JTC 1/SC 27.[2] Il s'agit d'une spécification prévue pour un Système de gestion de la sécurité de l'information (SGSI). Un SGSI est une approche systématique de gestion des informations sensibles de l'entreprise visant à en maintenir la sécurité. Il englobe les personnes, les procédures et les systèmes informatiques à travers l'application d'un processus de gestion des risques.
3	Loi de 2000 relative aux technologies de l'information	<p>La loi relative aux technologies de l'information (Loi TI) est une loi visant à accorder une reconnaissance juridique aux opérations effectuées par le biais d'échanges de données électroniques et d'autres moyens de communication électronique, communément connus sous le nom de « commerce électronique », qui impliquent l'utilisation de méthodes de communication et de stockage des informations alternatives au papier dans le but de faciliter le dépôt électronique des documents auprès des agences gouvernementales et de modifier par ailleurs le Code pénal indien, la loi indienne sur la preuve de 1872 (<i>Indian Evidence Act</i>), la loi sur la preuve des livres bancaires de 1891 (<i>Bankers' Books Evidence Act</i>) et la loi sur la Banque centrale d'Inde de 1934 (<i>Reserve Bank of India Act</i>). Elle accord également cette reconnaissance à des questions qui leur sont connexes ou accessoires. La Loi de 2000 relative aux technologies de l'information aborde les questions suivantes :</p> <ol style="list-style-type: none"> 1. La reconnaissance juridique des documents électroniques ; 2. La reconnaissance juridique des signatures numériques ;

		<p>3. Les infractions et contraventions ;</p> <p>Les systèmes d'exercice de la justice en matière de cybercriminalité.</p>
4	Accords de non-divulgation (<i>Non-Disclosure Agreements</i> , NDA)	Un NDA est un Accord ou une convention de confidentialité créant une obligation juridique à l'égard du respect de la vie privée et obligeant ceux qui en conviennent de garder toutes les informations données en sécurité ou secrètes.
5	SFTP	Le protocole sécurisé de transfert de fichiers (<i>Secure File Transfer Protocol</i> , SFTP) est un protocole réseau qui fournit des fonctionnalités d'accès, de transfert et de gestion des fichiers sur tout flux de données fiable.
6	XML	Le XML (<i>Extensible Markup Language</i>) est un langage de balisage définissant un ensemble de règles de codage des documents dans un format lisible par l'homme et par la machine. Le XML constitue un moyen souple de créer des formats d'information communs et de partager ce format et ses données sur le Web, les intranets et ailleurs. Le XML a été créé pour structurer, stocker et transporter des informations. Si l'utilisation du XML concerne avant tout les documents, il est largement utilisé pour représenter des structures de données arbitraires, notamment dans les services Web.