WCO GUIDELINES FOR STRENGTHENING COOPERATION AND THE EXCHANGE OF INFORMATION BETWEEN CUSTOMS AND TAX AUTHORITIES AT THE NATIONAL LEVEL

V. Developing a Memorandum of Understanding/Agreement (MOU/MOA)

ii. India

Data Sharing Policy

Central Board of Excise and Customs (CBEC)

Data Sharing Policy

February 2015

1. Introduction

Data is universally recognized as a valuable resource that should be maintained in a manner which ensures that its potential value is optimally realized. Most data today is maintained and exchanged electronically, which has increased the ease of exchange of data and at the same time increased the need for a structured and secure mechanism for such an exchange. India's National Data Sharing and Accessibility Policy (NDSAP) states *inter alia* that the principles on which data sharing and accessibility need to be based include: Openness, Flexibility, Transparency, Protection of Intellectual Property, Formal responsibility, Professionalism, Interoperability, Quality, Security, Efficiency, Accountability, Sustainability and Privacy. There is a large quantum of data generated at the cost of public funds by various organizations and institutions in the country and this data can be used for scientific, economic and developmental purposes.

2. Need for Data Sharing Policy

2.1 Current Status

The Central Board of Excise and Customs (CBEC) has a rich repository of taxpayer data pertaining to Customs, Central Excise and Service Tax. The Directorate of Systems (DoS), CBEC holds this data in its IT systems in a Custodial capacity. Online transactional data pertaining to Customs, Central Excise and Service Tax resides in the respective business applications, namely, ICES, ACES, ICEGATE, etc. The centralization of its consolidated IT Infrastructure has also enabled CBEC to create an Enterprise Data Warehouse (EDW) which is also actively being used to address the data requests of both internal and external agencies.

There has been an increasing demand by several external agencies that the data which is collected with the deployment of public funds should be made readily available to all for enabling rational debate, better decision-making, policy formulation and use in meeting civil society needs.

Currently, data is being shared with multiple internal and external agencies within India, in different ways and modalities. CBEC's ICEGATE application serves as the interface for providing Customs transactional data to agencies such as DGFT, DGCIS,

RBI, etc. Data from the Enterprise Data Warehouse is being increasingly used for answering Parliament questions and for framing responses to applications received under the Right to Information (RTI) Act. The details of such exchange with external and internal agencies within India are tabulated at Annex-A and Annex-B respectively.

Data to external entities is shared using either of the following modes:

1. On official or government email ids
2. Secure file transfer protocol (SFTP) - particularly in cases where the data file size is large and cannot be sent as simple mail attachments
3. Over Virtual Private Network (VPN) to identified trusted external users for pre-agreed reports

2.2 Need for Policy

CBEC holds indirect tax data in a Custodial capacity. As discussed above, the data requests from the external users have increased very significantly. In addition, since 2011 CBEC has adopted the ISO 27001 standard for information security for which it is audited every year by Standards Testing Quality and Certifications, a body under the Ministry of Information and Communication Technology (MICT) for compliance. This standard which has been revised in 2013 has a specific domain of communications security where stringent guidelines have been laid down for Information Transfer within an organization and with any external entity. The relevant extract is placed at Annex-C.

This needs to be seen in the context of increasing demands for data in view of increasing awareness of the value and benefits that such data brings, which include:

1. Maximising use of Government's data for the benefit of stakeholders
2. Improving policy making across government
3. Supporting research by various government bodies/ research agencies
4. Detection of potential frauds
5. Non-intrusive profiling of taxpayers

Also, while some exchanges, such as those between ICEGATE and DGFT & DGCIS are structured and well established, most of the others are in the nature of ad-hoc requests and there is a need to bring structure and rigour to the process for entertaining requests for data and providing such data.

All the above make it imperative for CBEC to formulate a Data Sharing policy along with a protocol for exchange of data with external entities within India. In course of time, a similar protocol for exchange of data with external entities outside India may also have to be established.

The key aspects to be covered in the data sharing policy include:

- Scope and Applicability
- Data Categorisation
- User Categorisation
- Request Categorisation and Modality of data sharing
- Funding for Data Sharing
- Data Storage and Retention
- Reciprocity Clause
- Saving Clause

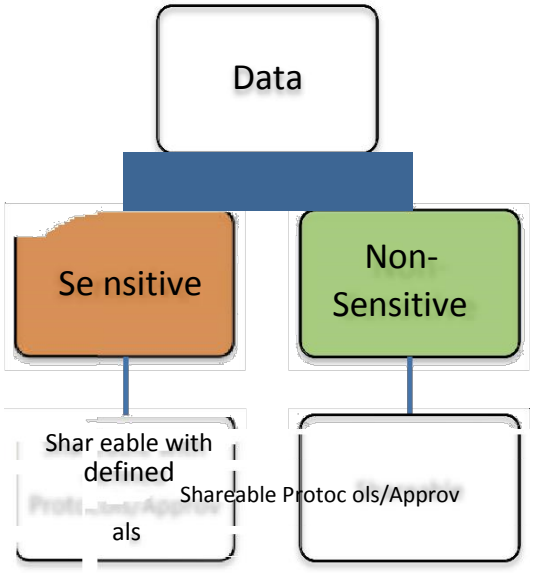
2.3 Scope and Applicability

This document lays down the policy governing information exchange between CBEC and external agencies within India.

As regards data exchange with external agencies outside India, subject to approval from the competent authority with duly identified data content, the same shall be governed by a separate self contained document ***CBEC's IT Connectivity Protocol with Foreign Entities.***

While the applicability of this policy is primarily focused on the Directorate of Systems, CBEC (since most data is exchanged electronically), its applicability to CBECs field offices and other Directorates would also need to be laid down, especially in view of Trade bodies' concerns regarding availability of sensitive commercial data in public domain.

3. Data Categorisati on



The data available with CBEC is categorised for shareability bas ed upon its sensitivity, granularity, cri ticality and ownership/data origination. In line with the categorization of data pres cribed in NDSAP, data is then classified as S hareable and Non-shareable. As can be seen from the diagram above, CBEC data el ements have been categorised as Sensit ive and Non-Sensitive. Data falling under t he Sensitive category shall ordinarily be provided against a specific authorized reque st on a case to case basis and backed with a Non-disclosure Agreement between the requestor and CBEC. For regular/periodic requests for data, the requestor shall enter into a MoU (Annex-G) and Non-di sclosure Agreement for such data with CBEC.

3.1 Sensitive

The following categories of data shall be treated as Sensitive:

3.1.1. Sensitive Personal Information (SPI) and Personally Identifiable Information (PII): As per the Information Technology Act 2000 (as amended in 2008), Sensitive Personal Information (SPI) and Personally Identifiable Information (PII) data is Highly Sensitive. All data pertaining to an individual entity shall therefore be classified as Sensitive.

3.1.2. Commercially sensitive information that has financial implications for a taxpayer: Data which if compromised, can cause economic impact to a taxpaying entity such as invoice details, pricing information, supplier details, etc shall be classified as sensitive.

3.1.3. Data that comes into existence through enforcement functions of CBEC: Data generated as part of internal analysis using CBECs internal tools and techniques for profiling as part of Enforcement functions, Risk Analysis, Investigations and Intelligence gathering etc shall be considered as Sensitive. This includes data contained in DRIPS, Offence data, RMS Interdiction details.

3.1.4. Data pertaining to the configuration/technology of CBEC's IT systems

3.1.5. Granular data pertaining to an individual's access/activity logs in the system and such other forensic data which is available in CBEC's IT systems

3.1.6. Data provided to CBEC by another Government organisation in India or any other organization through an existing arrangement (eg IEC data from DGFT) or with whom CBEC has executed a MoU/NDA will fall in the Sensitive category.

3.1.7. Third party granular transactional data: Third party granular transactional data contained in individual import/export documents, returns, payments etc shall ordinarily be treated as Sensitive data,

having regard to its commercial sensitivity. Thus, while the granularity of information contained in such a data may not enable a direct identification of a Commercial entity, yet such data could be related to manufacture of specific commodities in a particular area, or the valuation trends of a commodity imported from a particular country of origin- the information contained herein would still be sensitive from a perspective of commodity level profiling of imports as well as domestic production.

3.1.8. Information/data received under International Treaty/Agreements shall also be classified as Sensitive data.

3.2 Non-Sensitive Data

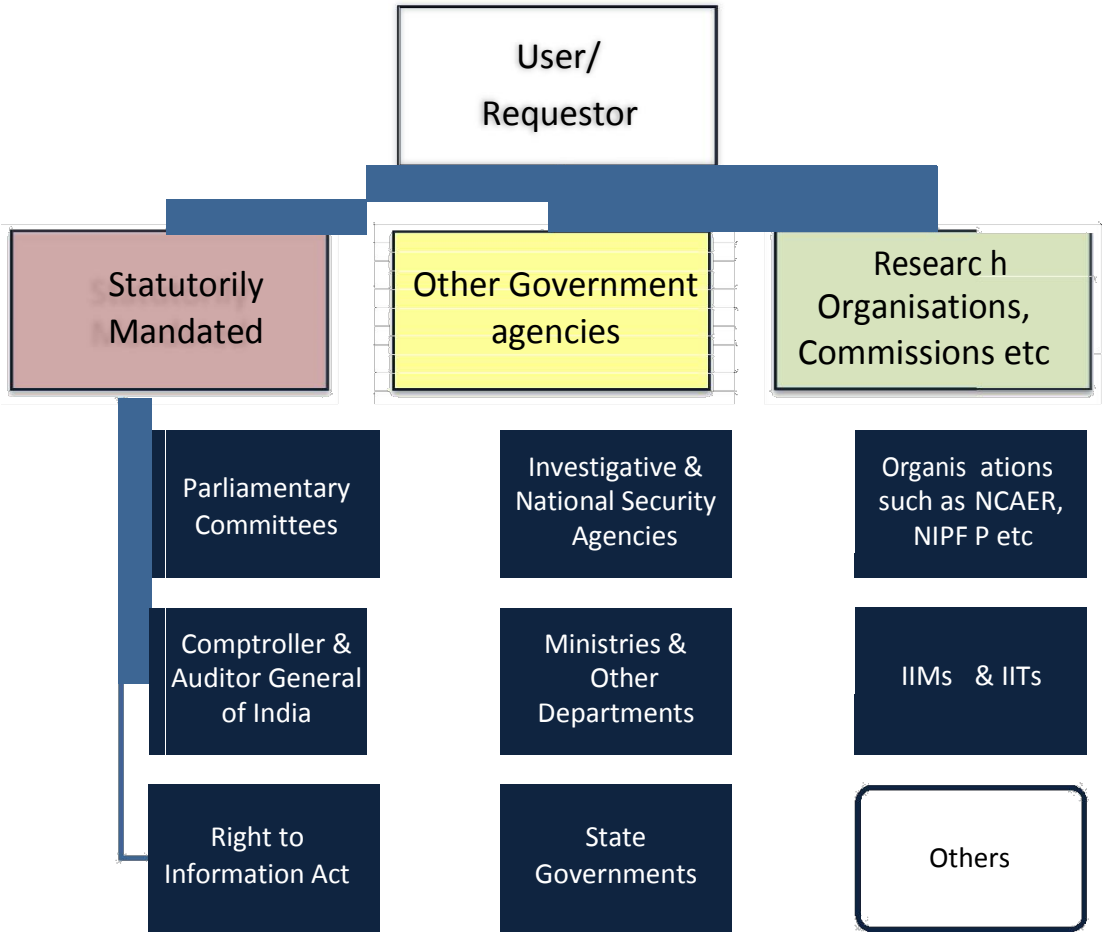
Highly summarized or aggregated data created by combining information on individuals and legal entities shall be considered as Non-Sensitive. Data which is mandated by Statute, other Acts in force and/or policy decisions by the Board to be publically displayed or openly hosted on CBEC website/s shall be treated as falling into this category.

Data which is placed on CBEC's website in compliance with the RTI Act and long standing agreements/practice such as the Daily Trade Report (DTR) etc shall also fall into this category.

CBEC may, at its discretion, decide to openly publish any data which it feels is required in the interest of transparency or public good.

As regards the modalities of sharing such Non-Sensitive data for which requests are received by the CBEC, the modalities would be governed by the process prescribed for servicing of ad-hoc data requests. Thus, an entity requesting for Non-Sensitive data would be required to send the data request in the prescribed template (Annex-E) and indicate the name of the person duly authorised to receive the data and once the request is processed, CBEC shall ordinarily transmit the data to the requestor's official e-mail ID.

4. User Categorisatio n



The diagram above depicts the categorisation of requestors of data from CBEC. There are broadly three categories as under:

4.1 Statutorily Mandated

This category includes agen cies or bodies empowered by Statute to ask for data such as Parliamentary Committees, the Comptroller & Auditor General of India and offices there under (eg CERA) an d applicants under the ambit of the Right to Information Act. Requests under this c ategory would be accorded the highest priority and dealt with accordingly. Data falling under the Sensitive category shall ordinarily be provided against a specific authorized request on a case to case basis and backed with a Non-disclosure Agreement between the requestor and CBEC. For

regular/periodic requests for data, the requestor shall enter into a MoU (Annex-G) and Non-disclosure Agreement for such data with CBEC.

4.2 Other Government Agencies

This category would cover other Government agencies/bodies such as National Security Agencies, Investigating Agencies outside CBEC, other ministries and departments, State Government departments etc. Sensitive data may be provided against a specific authorized request on a case to case basis and backed with a Non-disclosure Agreement between the requestor and CBEC. For regular/periodic requests for data, the requestor shall enter into a MoU (Annex-G) and Non-disclosure Agreement for such data with CBEC.

4.3 Research Organisations, Commissions etc

This category would cover requests from academic and research institutions such as National Council of Applied Economic Research (NCAER), National Institute of Public Finance and Policy (NIPFP), Indian Institutes of Management (IIMs) and Indian Institutes of Technology (IITs) etc. It would cover requests from specially set up Commissions or Task Forces etc. Requests from such organisations would ordinarily be entertained for non-sensitive data only. In the event that a specially set up Commission/Task Force seeks Sensitive data, CBEC would examine each request on its own merit and decide whether such data can be provided. In the event that CBEC decides to provide such data, all conditions for sharing sensitive data such as MoU and Non-disclosure Agreement shall apply. In addition, such requests would be taken up only after pending requests under the priority category have been dealt with.

5. Request Categorisation and Modality of Data Sharing

Data sharing modality would depend upon the data categorization and data volume. Data requests would be categorised into:

i. Ad- hoc request based

ii. Structured periodic exchange of identified data.

5.1 Ad-hoc Request-Based

Under this category, data will be shared on the basis of a specific request for the same. It would cover requests which seek a limited amount of data for a specific entity and is related to an organizational requirement, an investigation or inquiry. All requests will be entertained only when sent in the prescribed template (Annex- E). This template would be available on CBEC's website www.cbec.gov.in

In case the data pertains to an investigation/inquiry being conducted by a law enforcement agency, CBEC may consider providing such data to a person duly authorised by the said agency.

In each such case where this request is fulfilled by the Directorate of Systems, the data shall be provided only with the approval of Director General (Systems).

In such cases data shall ordinarily be provided over requestor's official e-mail in response to the data request template at Annex- E received either over e-mail or preferably in hard copy. In case it is found that the e-mail so received has not come from a proper domain or is detected to be a malicious e-mail, CBEC reserves the right to take such action including forensic investigation by third party auditors and /or legal remedy, as may be required. If malicious intent is established, CBEC at its discretion may choose not to provide any further data to the said entity

5.2 Structured Exchange of Identified Data

This category would pertain to data required to be exchanged in agreed structured formats at a defined frequency, including bulk data sharing.

Organisations seeking data under this category would be required to execute a formal MoU and a Non-disclosure Agreement which will govern this sharing of data. Additionally they would be required to nominate a nodal officer and an alternate nodal officer who would be the authorized contact person for data transmission and communication related to the same.

Data under this category would ordinarily be exchanged through a secure electronic mechanism. In due course, it would be CBEC's endeavour to secure such exchange through Digital Signatures whether personal or server level.

6. Funding For Data Sharing

CBEC reserves the right to levy such nominal fees as may be necessary to cover the costs of generating data in specific customised formats. Such levies would be determined after due approval process from the Competent Authority and as per applicable Government policies. Currently CBEC is not charging anything for providing data, regardless of its complexity or size.

7. Data Storage and Retention

Sensitive data provided by CBEC under this policy should be stored on a secure system whereby access is restricted to only authorised personnel. The data should be retained only until it has served the purpose for which it was obtained and securely erased thereafter. Any/all liability arising out of disclosure of such data shall lie solely with the requesting organisation.

8. Reciprocity Clause

The Government agencies, research organisations, etc seeking information/ data from CBEC would be bound to share data owned by them and requested of them by CBEC should there be a requirement of the same. The reciprocity clause would be made part of the MoU/Agreement that CBEC would be entering into with the said agencies/ organisations for sharing data with them.

9. Saving Clause

Any organization/entity that receives data from CBEC under this policy assumes all legal liability arising out of any precipitative action taken by such organization/entity based on this data.

The recipient of the data shall ensure that data containing information specified to be confidential by CBEC or agreed mutually to be confidential between CBEC and the recipient are maintained in confidence and are not disclosed or transmitted to any unauthorized persons nor used for any purposes other than those intended by the parties. When authorized, further transmission of such confidential information shall be subject to the same degree of confidentiality.

Shared Data shall not be regarded as containing confidential information to the extent that such information is in the public domain. CBEC and the recipient may agree to use a specific form of protection for data such as a method of encryption to the extent permitted by law.

10. Annex A- Current Data Exchange with External Agencies

S No	Transfer Type	Source Application	Target Application (Internal) / Agency (External)	Scripts or Directly through Application/Database	Type of Data	Frequency	Mode of Transmission	Transfer Mode (Dump/E-mail /SFTP/CD
1	Near Real Time	ICES	EICI	Scripts	Directory dump of selected directories	Once in every day at 06:30 am	Automated	Public SFTP
2	Near Real Time	ICES	SEZ Online	Scripts	Directory dump of selected directories	As on demand	ICEGATE	Public SFTP
3	Periodic	ICES	CAG	Scripts	ICES Imports / Exports dump - Financial	As on demand	SI/ICES	Through CD

S No	Transfer Type	Source Application	Target Application (Internal) / Agency (External)	Scripts or Directly through Application/Database	Type of Data	Frequency	Mode of Transmission	Transfer Mode (Dump/E-mail /SFTP/CD
					year wise			
4	Near Real Time	ACES	EASIEST (NSDL)	Direct through Application	Assessee registration data	Twice in a day at 8am and 8 Pm	Automated	Public SFTP
5	Near Real Time	EASIEST (NSDL)	ACES	Direct through Application	E-payment data	Twice in a day at 7am and 7 Pm	Automated	Public SFTP
6	Real Time	ICEGATE	Institutional Partners	Direct through Application	With banks for Challan Data, Custodian Messages, with DGFT	Real time	Automated	Public SFTP
7	Near Real	EASIEST (NSDL)	EDW	Direct through Application	E-payment data	Twice in a day at 7am and 7 Pm	Automated	Public SFTP

S No	Transfer Type	Source Application	Target Application (Internal) / Agency (External)	Scripts or Directly through Application/Database	Type of Data	Frequency	Mode of Transmission	Transfer Mode (Dump/E-mail /SFTP/CD
	Time							
8	Ad-Hoc	RBI	ICES/ICEGATE	Scripts	AD Code Dump	Adhoc provided by RBI for uploading in ICES	RBI (Manual)	By E-mail
9	Ad-Hoc	CBDT	CBEC	Scripts	PAN data , returns and payments	As on demand	CBDT (Manual)	Public SFTP
10	Ad-Hoc	CBEC	MCA	Scripts	Company registration and returns data	As on demand	MCA (Manual)	Public SFTP
11	Periodic	DGFT	ICEGATE	Direct through Application	License details, IEC	Hourly basis by ICEGATE	Automated	Public SFTP

S No	Transfer Type	Source Application	Target Application (Internal) / Agency (External)	Scripts or Directly through Application/Database	Type of Data	Frequency	Mode of Transmission	Transfer Mode (Dump/E-mail /SFTP/CD
12	Ad-Hoc	ICEGATE	DGCIS	Direct through Application	Daily SB and BE details after ooc and LEO	once in a day by ICEGATE	Automated	Public SFTP
13	Real Time	ICEGATE	DGFT	Direct through Application	Exporter wise shipping bill details	ICEGATE - to be checked	Automated	Public SFTP
14	Periodic	EDW	DEA		Import Details of Gold	Weekly/Monthly		E-mail
15	Periodic	EDW	Ministry of Petroleum		Custom imports; transactional level for	2-3 months		E-mail

S No	Transfer Type	Source Application	Target Application (Internal) / Agency (External)	Scripts or Directly through Application/Database	Type of Data	Frequency	Mode of Transmission	Transfer Mode (Dump/E-mail /SFTP/CD
					Liquified Natural Gas (LNG)			
	Periodic	EDW	Directorate General of Anti-Dumping (Ministry of Commerce)		Custom imports; transactional level	Monthly		E-mail

Note:- The EDW team has been providing data on ad-hoc basis with the approval of DG (Systems) to External Agencies such as the Comptroller and Auditor General of India, Ministry of Statistics and Programme Implementation, National Council of Economic and Applied Research, National Institute of Public Finance and Policy, VAT Departments of Gujarat and Punjab, the Rubber Board of India, Shah Commission, Tax Administrative Reforms Commission etc.

11. Annex B- Current Data Exchange with Internal Agencies

S No	Transfer Type	Source Application	Target Application (Internal) / Agency (External)	Scripts or Directly through Application/ Database	Type of Data	Frequency	Mode of Transmission	Transfer Mode (Dump/E-mail /SFTP/CD
1	Near Real Time	ICES	DRI	Scripts	Oracle Export dump for 1. On Submission BE and SB 2. End of Day after OOC and LEO 3. End of day IGM data 4. Monthly directory dumps for 14 directories	1. On Submission every 2 hours 2. EOD data - Once in a day 3am/4am 3. EOD Data - Once in a day - 4am 4. Monthly on every 1st day at 7 am	Automated	DRI SFTP
2	Near Real Time	ICES	ACES	Scripts	IEC data	Every Day at 6:30 am	Automated	SFTP
3	Near Real Time	ICES	Custom Duty Calculator	Scripts	Directory dump of selected directories	Every Day at 6 am	Automated	Public SFTP
4	Near Real Time	ICES	ICEGATE Web site	Scripts	Daily revenue data (Daily list)	Once in a day at 7 am	Automated	SFTP / Web site
5	Near Real	ACES	ICES	Scripts	ST refund data	Every day at 00:30	Automated	SFTP

S No	Transfer Type	Source Application	Target Application (Internal) / Agency (External)	Scripts or Directly through Application/ Database	Type of Data	Frequency	Mode of Transmission	Transfer Mode (Dump/E-mail /SFTP/CD
	Time							
6	Periodic	ACES	EDW	Directly	DR Database for differential data	Once in Fortnight	Automated	Database
7	Periodic	ICES	EDW	Directly	DR ICES Database for differential data	Every Day morning	Automated	Database
8	Periodic	ICES	DRI, CBEC	Scripts	Onion, wheat and Rice report	Weekly - Every Monday	SI (Manual)	By E-mail
9	Periodic	ICES	DRI, CBEC	Scripts	Monthly revenue report - Site wise	Monthly - on every 1st of month	SI (Manual)	By E-mail
10	Periodic	ICES	ICEGATE	Scripts	Total BE and SB filing site wise	Every Day at 8 am	Automated	By E-mail
11	Periodic	EDW	TRU		Import details of Gold and Silver, Data pertaining to Pol/Non-Pol commodities	Monthly		By E-mail
12	Periodic	EDW	Chairperson, CBEC's Office		Central Excise Revenue Reports	Monthly		By E-mail
13	Periodic	EDW	Commissioner (Customs & Export Promotion)		Import Details under various Free Trade Agreements (FTAs)	Quarterly		By E-mail

Note:- The EDW team has been providing data on ad-hoc basis to internal formations such as Commissionerates, Directorate of Revenue Intelligence, Directorate General of Central Excise Intelligence, Directorate General of Valuation, Directorate General of Audit etc

12. Annex C- ISO 27001/27002

Domain 13 of ISO/IEC 27001:2013 & 27002 (Implementation Guidelines)

13 Communications Security

13.1 Network Security Management

13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 Information transfer policies and procedures

Control

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Implementation guidance

The procedures and control to be followed when using communication facilities for information transfer should consider the following items:

a) procedures designed to protect transferred information from interception, copying modification, mis-routing and destruction;
b) procedures for the detection of and protection against malware that may be transmitted though the use of electronic communication (see 12.2.1);
c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;
d) policy or guidelines outlining acceptable use of communication facilities (see 8.1.3);
e) personnel, external party and other user's responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing etc.;
f) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information (see Clause 10);
g) retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulation;
h) control and restriction associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;
i) advising personnel to take appropriate precautions not to reveal confidential information;

j) not leaving messages containing confidential information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing;
k) advising personnel about the problems of using facsimile machines or services, namely :

1) unauthorized access to built-in message stores to retrieve messages;
2) deliberate or accidental programming of machines to send message to specific numbers,
3) sending documents and messages to the wrong number either by misdialing or using the wrong stored number.

In addition, personnel should be reminded that they should not have confidential conversation in public places or over insecure communication channels, open offices and meeting places.

Information transfer services should comply with any relevant legal requirements (see 18.1).

Other information

Information transfer may occur through the use of a number of different types of communication facilities, including electronic mail, voice facsimile and video.

Software transfer may occur through a number of different mediums, including downloading from the Internet and acquisition from vendors selling off-the-shelf products.

The business legal and security implication associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls should be considered.

13.2.2 Agreements on information transfer

Control

Agreement should address the secure transfer of business information between the organization and external parties.

Implementation guidance

Information transfer agreement should incorporate the following:

a) management responsibilities for controlling and notifying transmission, dispatch and receipt;
b) procedures to ensure traceability and non-repudiation;
c) minimum technical standards for packaging and transmission;
d) escrow agreements;

e) courier identification standards;
f) responsibilities and liabilities in the event of information security incidents, such a loss of data;
g) use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected (see 8.2);
h) technical standards for recording and reading information and software;
i) any special controls that are required to protect sensitive items, such as cryptography (see Clause 10);
j) maintaining of chain of custody for information while in transit;
k) acceptable levels of access control.

Policies, procedures and standards should be established and maintained to protect information and physical media in transit (see 8.3.3), and should be referenced in such transfer agreements.

The information security content of any agreement should reflect the sensitivity of the business information involved.

Other Information.

Agreements may be electronic or manual, and may take the form of formal contracts. For confidential information, the specific mechanisms used for the transfer of such information should be consistent for all organization and types of agreements.

13.2.3 Electronic messaging

Control

Information involved in electronic messaging should be appropriately protected.

Implementation guidance

Information security considerations for electronic messaging should include in following:

a) protecting message from messages from unauthorized access, modification or denial of services commensurate with the classification scheme adopted by the organization;
b) ensuring correct addressing and transportation of the message;
c) reliability and availability of the services;
d) legal considerations, for example requirements for electronic signatures;
e) obtaining approval prior to using external public services such as instant messaging, social networking or file sharing;
f) Stronger levels of authentication controlling access from publicly accessible networks.

Other information

There are many types of electronic messaging such as email, electronic data interchange and social networking which play a role in business communications.

13.2.4 Confidentially or non-disclosure agreements

Control

Requirement or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentially or non disclosures agreement are applicable to external parties or employees of the organization. Elements should be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a) a definition of the information to be protected (e.g. confidential information);
b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;
c) required actions when an agreement is terminated;
d) responsibilities and actions of signatories to avoid unauthorized information disclosures;
e) ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;
f) the permitted use of confidential information and rights of the signatory to use information;
g) the right to audit and monitor activities that involve confidential information;
h) process for notification and reporting of unauthorized disclosure or confidential information leakage;
i) terms for information to be returned or destroyed at agreements cessation.
j) expected actions to be taken in case of a breach of the agreement.

Based on an organization's information security requirement, other elements may be needed in a confidentially or non disclosure agreement.
Confidentiality and non-disclosure agreement should comply with all applicable laws and regulations for the jurisdiction to which they apply (see 18.1)
Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

Other information

Confidentiality and non-disclosure agreements protect organizational information and inform signatures of their responsibility to protect, use and disclose information in a responsible and authorized manner.

There may be need for an organization to use different forms of confidentiality or non-disclosure agreements in different circumstances.

13. Annex D- IT Connectivity Protocols

Establishing Data Exchange

Table below provides **requirements towards enabling electronic data** exchange with CBEC:

S.No	Parameter	Modality
1	**Connectivity**	No direct connectivity to CBEC's production servers shall be allowed to any international partner. Message exchange would take place through placing of files in designated directories (separate Inbound & Outbound), with specific permissions
2	**Network Connectivity**	The default mode for establishing communication shall be over Site-to-Site SSL VPN
3	**Static IP Address**	Only authorized devices with declared static IP address/ Mac address shall be allowed access
4	**Network Port for incoming data**	Only specified port shall be allowed for communication
5	**Authentication**	Digital signature based authentication using Class III digital certificates TACACS/ CHAP
6	**Encryption**	ISAKMP (Internet Security Association and Key Management Protocol);AES;AS2;SHA
7	**File type**	Text file and XML formats
8	**Max File Size**	Only one file shall be accepted for each transaction The maximum permissible size of such file shall be 10KB
9	**Hash Function**	Hashing shall be implemented to check integrity of the files being exchanged - SHA
10	**Non-Disclosure and or Acceptable Use Agreement**	An agency connecting to CBEC's IT Systems will execute a mutually agreed agreement for non-disclosure and/or acceptable use of CBEC's data,

S.No	Parameter	Modality
		including its storage and archival.
11	**Audit Logs**	Audit logs will be created for each transaction and user activity. These may be subject to third party audits commissioned by CBEC.
12	**Other**	Tools that do not support logging or establishing forensic trails (including but not limited to Winscp) shall not be used by either party.

Communication Server: CBEC shall create separate Inbound and Outbound directories on its communication server; the files sought to be sent to the International partner shall be placed in the outbound directory by CBEC. Similarly the files sought to be received from the International partner shall be placed in the inbound folder by the International partner**.**

Data Purging / Archival: Once a file has been successfully picked up from the inbound directory by CBEC's IT Systems, it will be purged within an agreed timeframe not later than 7 days.

Communication Channel: It is important that both parties maintain clear lines of communication and towards this objective, both parties shall provide to each other the contact details of the Officer(s) In-charge of the data exchange, including the emergency contact details. Instance/s of planned and un-planned downtime shall be communicated to the other party**.**

Incident Response Protocol: Both the parties shall notify each other of intrusions, attacks, or misuse of data. In the case of a security breach, both parties shall coordinate their incident response activities.

Change Management

In the event of any updates to CBEC's IT Security policy and procedures, the corresponding update in the data exchange protocol shall be notified to the International partner. Thereafter, the updated protocol shall be treated as a

mandatory requirement for the data exchange between CBEC and the International partner.

Discontinuing the Data Exchange

- **Planned discontinuation**: In case discontinuation of the data exchange is warranted, the initiating party shall notify the other party in writing, and it shall in turn receive an acknowledgment for the same. The notification should describe the reason/s for the disconnection and provide the timeline for the disconnection

- **Emergency discontinuation**: If one or both parties detect an attack or any other contingency that exploits or jeopardizes the IT systems or data, data exchange can be terminated without providing a prior written notice to the other party. However, if such an action is warranted, the same shall be notified to the other party at the earliest thereafter.

Any of above requirements can be modified through the approval of the Chief Information Security Officer (CISO) of CBEC

14. Annex E- Request Based Template

TEMPLATE FOR DATA REQUESTS BY EXTERNAL AGENCIES IN INDIA		
S.No.	Particulars	Description
1	Name of the Requesting Organisation	
2	Mandate for seeking data (Whether Statutory/ MoU/Agreement etc)	
3	Name of the Requestor – Single Point of Contact (SPOC)	
4	Designation of the Requestor	
5	Requestor's official e-mail ID	
6	Requestor's direct contact No.	
7	Requestor's official address	
8	Data Requested – whether Customs/Central Excise/Service Tax	
9	Brief Description of purpose	
10	Data Elements Requested (Source of Element, if any. For example:Registration/Returns/Payments etc.)	
11	Customs/Central Excise Tariff Head (if applicable)*	
12	Time Period for which data requested	
13	Format of Report, if any	
14	Additional Requirements, if any	

*Non-provision of the Tariff Head would lead to delay in provision of the data

UNDERTAKING *(Not required in case of a valid MoU with CBEC)*

I/We..... (Name of the Organisation) hereby state that the data requested above is required for official purposes only and I/we undertake to ensure that I/we shall accord as high a degree of security and confidentiality as we do to our own organisation's secure data. I/We also hereby undertake that I/we shall not further share the data provided by CBEC without taking CBEC's concurrence in writing. I/We further undertake to assume all legal liability arising out of any precipitative action taken by my organization/entity based on the data received from CBEC.

I/We …… (Name of the Organisation) further undertake that we would be bound to share data owned by us as and when requested for by CBEC.

Signature.....

Name.....

Place.....

Date.....

For CBEC's Internal Use

Request Acknowledgement No.....
(S.No/DDmonYYYY; eg 1/01jan2014)

Request Received Date.....

Directorate of Systems File No., if any.....

Request Ticket No. (System generated), if any.....

Request Approved by.....

Request Approval Date.....

Date of completion of request.....

Mode of transmission (Tick as applicable):

- On official e-mail ID
- Through Secure FTP

- On media (with approval)
- In hard copy

15. Annex F- Proposed Data sharing process

1. All data requests to the Directorate of Systems should follow the following process:

    a. Head of the requesting agency should write to the CBEC providing the details of the request like the purpose of the data request, data fields required and the periodicity of the data sought. He would also appoint a Single Point of Contact (SPoC) for their department who would interact with the relevant officials of the DG Systems and convey his contact information (address, telephone number, fax and official e-mail id on NIC or other government domain) for further correspondence. Future separate or supplemental data requests from the same office could be sent to Directorate of Systems by the SPoC via either letter or e-mail.

2. The request for data retrieval/analysis addressed to CBEC from External agencies would have to be first approved in principle by the Project Manager (EDW Project), CBEC before the feasibility of provisioning the data can be examined by the EDW team.

3. Feasibility of provisioning the data requested would then be undertaken by the EDW team and they may contact the SPoC of the office requesting data for any clarifications required with approval from the Project Manager (EDW Project), CBEC.

4. In case the data retrieval is not feasible, then the requesting agency would be immediately informed about the same.

5. Once the data has been retrieved/analysed, the data has to be shared with the Project Manager (EDW Project), CBEC for review.

6. After the review and corrections in the data, if any, the approval for sending the data would be required in writing from the DG (Systems) through the concerned ADG.

7. The data shall be sent only to the official e-mail ID of the SPoC (preferably NIC) of the office requesting for data.

8. In case the data is large in size, the data shall be transferred to the concerned officer via SFTP (secured File Transfer Protocol). The modality of such SFTP will be governed by the methodology in Annex-D

9. Usually no data shall be extracted on a portable media (CD, pen drive etc.). Exceptions to this rule may be considered only after approval by DG (Systems).

10. All responses to the SPoC of the office requesting data after EDW Project Manager's approval shall be routed through the EDW helpdesk.

11. In case any data request by an External Agency is routed through a CBEC office then it would be treated as an internal request and response to the same would be sent to the concerned CBEC official.

12. Logs of all the External data requests, correspondences/e-mails relevant thereto, and soft copies of data furnished would be kept with the EDW team for records.

13. The steps mentioned above shall be followed for all Data Requests received from External Agencies. Any deviation from the same under exceptional circumstances may only be made with the due approval of the DG (Systems).

16. Annex G- Draft MoU

MEMORANDUM OF UNDERSTANDING

BETWEEN

CENTRAL BOARD OF EXCISE AND CUSTOMS, MINISTRY OF FINANCE, GOVERNMENT OF INDIA

&

_____

FOR

EXCHANGE OF DATA FOR IMPROVING TAX COMPLIANCE

This MoU made this _____ th/rd day of _____

BETWEEN

Central Board of Excise and Customs (CBEC), Department of Revenue, Ministry of Finance, Government of India and represented by ***Director General, Directorate of Systems (DOS), Customs & Central Excise***, and/or person/s authorized by CBEC in writing to represent it in this regard, herein after referred to as "CBEC" (which expression shall unless excluded by or repugnant to the context deemed to include its successor/s in office or assign) or party of the FIRST PART.

AND

_____ and/or person/s authorized by _____ in writing to represent it in this regard, herein after referred to as _____ (which expression shall unless excluded by or repugnant to the context deemed to include its successor/s in office or assign) or party of the SECOND PART.

Whereas It has been agreed that there needs to be a structured mechanism for regular exchange of identified data fields between CBEC and _____ for _____ (purpose of signing the MoU) this Memorandum of Understanding (MoU) is hereby executed by parties of the first and second part:

Article 1
Object and Scope

1.1 The "Memorandum of Understanding", hereinafter referred to as "the MoU", specifies the terms and conditions under which the parties will exchange data.

1.2 The MoU consists of the provisions set out as under and shall be completed by the Annexures, which will form an integral part of this MoU

1.3 Unless otherwise agreed by the parties, the exchange of data shall be in secure electronic mode.

Article 2
Definitions

For the purpose of the MoU, the following terms are defined as follows:

2.1 Transmitting Party: Party of the first or second part as the case may be, which is providing data

2.2 Receiving Party: Party of the first or second part as the case may be, to whom data is being provided.

2.3 Financial Year: A Financial Year is year in which income is earned and is a period of twelve months commencing from 1st April of a year to 31st March of the following year.

2.4 Assessment Year: Assessment year means the period of twelve months commencing on 1st April every year and ending on 31st March of the next year immediately following the Previous Year.

2.5 Business Day: A business day means any day except a Saturday, Sunday or any gazetted public holiday at the location of the Receiving Party.

2.6 LTU: A LTU is self-contained tax office under the Department of Revenue acting as a single window clearance point for all matters relating to Central Excise, Income Tax/ Corporate Tax and Service Tax.

Article 3
Validity and Conformity

3.1 The MoU is valid for period of three years and will be effective from _____ (Date).After the expiry of the validity, the MoU may be extended by mutual consent of both parties

3.2 Each Party shall ensure that the data sent or received is in conformity with the agreed formats and frequency as specified in Annexure

Article 4
Use of Exchanged Data in a Legal Proceeding

To the extent permitted by Indian law which may apply, the parties hereby agree that in the event of the data so exchanged being required to be produced in a court of law for a civil or criminal proceeding, the data relied upon shall be substantiated by documentary evidence and other statutory documents as applicable under the Customs Act, Central Excise Act, Service Tax Laws under Finance Act 1994 and any other law for the time being in force.

Article 5

Modality of Exchange and acknowledgement of receipt

5.1 Unless otherwise warranted data shall be exchanged in a secure electronic mode.

5.2 Unless otherwise warranted acknowledgement of receipt shall be sent electronically.

5.3 The Receiving Party shall ensure that an acknowledgement is sent to the transmitting Party within two business days of receipt of the data, unless an alternative time limit has been mutually agreed.

5.4 The Receiving and Transmitting Parties shall both maintain a Date & Time stamped record of the files transmitted and received.

Article 6

Security of Data Shared

6.1 The parties undertake to implement and maintain security procedures and measures in order to ensure the protection of data shared against the risks of unauthorized access, alteration, delay, destruction or loss.

6.2 Security procedures and measures may include the verification of origin, the verification of integrity, the non-repudiation of origin and receipt and the confidentiality of data shared. Where warranted, additional security procedures and measures may be expressly specified and mutually agreed.

6.3 If the use of security procedures and measures results in the rejection of, or in the detection of an error in the data shared, the receiver shall inform the sender thereof, within the specified time limit.

Where a rejected or erroneous data is retransmitted by the sender, the data should clearly state that it is a retransmission of corrected data.

Article 7

Confidentiality and Saving

7.1 The parties shall ensure that data containing information specified to be confidential by the sender or agreed mutually to be confidential between the parties, are maintained in confidence and are not disclosed or transmitted to any unauthorized persons nor used for any purposes other than those intended by the parties.

When authorized, further transmission of such confidential information shall be subject to the same degree of confidentiality.

7.2 Shared Data shall not be regarded as containing confidential information to the extent that such information is in the public domain.

7.3 The parties may agree to use a specific form of protection for data such as a method of encryption to the extent permitted by law.

7.4 A complete and chronological record of all shared data exchanged by the parties shall be stored by each Party, unaltered and securely, in accordance with the time limits and specifications prescribed by legislative requirements and in any event, for the duration of the MoU.

7.5 Any organization/entity that receives data from CBEC under this policy assumes all legal liability arising out of any precipitative action taken by such organization/entity based on this data.

Article 8

Reciprocity Clause

8.1 The Government agencies, research organisations, etc seeking information/ data from CBEC would be bound to share data owned by them and requested of them by CBEC should there be a requirement of the same. The reciprocity clause would be made part of the MoU/Agreement that CBEC would be entering into with the said agencies/ organisations for sharing data with them.

Article 9

Operational requirements for Data Exchange

9.1 The parties undertake to implement and maintain an operational environment to operate data exchange according to the terms and conditions of this MoU, which includes but is not limited to the following:

a. **Operational equipment**

The parties shall provide and maintain, the equipment, software and services necessary to transmit, receive, record, process and store the data shared.

b. **Mode of communication**

Unless otherwise specified, the default mode of communication in respect of operational matters related to data exchange shall be the official email of the persons authorized by the parties.

Article 10

Responsibilities of Parties

10.1 Responsibilities of Parties

Parties shall provide the following to facilitate the exchange of data:

i. Appoint nodal officer(s) to act as point of contact for coordinating the exchange of data.

ii. Accord due priority and resources for timely completion of tasks related to exchange of data.

iii. Establish a mechanism for resolving data quality issues, if any, within a reasonable timeframe.

iv. Establish a mechanism for periodic review of exchange of data and results thereof.

Article 11

General Terms and Conditions

11.1 No Commercial Consideration

The Parties mutually agree that there exist no commercial considerations in respect of this MoU.

11.2 Indemnification

CBEC and _____ agree to indemnify each other against consequential effects arising out of steps taken under this MoU.

11.3 Force Majeure (can be taken off as there is no commercial consideration here)

i. _____ and CBEC shall not be liable for failure to meet obligations due to Force Majeure.

ii. Force Majeure impediment is taken to mean unforeseen events, which occur after signing of this MoU including but not limited to strikes, blockade, war, mobilization, revolution or riots, natural disaster, acts of God, refusal of license by State/Central Government authorities, in so far as such an event prevents or delays the contractual Party from fulfilling its obligations.

iii. In case the Force Majeure conditions continue for more than 60 days, all the Parties shall discuss the effect of such conditions on the MoU and mutually decide the course of action to be followed.

A Party to this MoU cannot be sued in any Court of Law for being unable to perform as per the stipulations of the MoU due to circumstances beyond its control.

11.4 Deviations and Dispute Resolution

On all aspects where the above articles of understanding are silent, for special cases of deviation from these articles, the decision mutually agreed upon between _____ and CBEC will be final.

11.5 Dispute Resolution

In the event of any dispute relating to or arising out of this MoU, such dispute shall be resolved amicably by mutual consultation. If such resolution is not possible, then the unresolved dispute or difference shall be referred to a committee consisting of the Secretary (Revenue), Chairperson CBEC, _____ and any member co-opted by the other party, whose decision shall be binding on both Parties.

11.6 Exit Clause

Either of the parties can terminate this MoU by giving three-month notice to each Party as per mutually decided terms and conditions.

On expiry/termination of this MoU, any Party to the MoU shall not assume any responsibility/liability in any form – technical, legal, financial etc for any eventual consequences to the other Party, for events arising after such expiry/ termination.

11.7 Amendment to MoU

No verification in or modification of the terms of this MoU shall be made except by written amendment signed by both the parties

IN WITNESS WHEREOF the parties have executed in duplicate on the day and year, hereinafter indicated.

FOR AND BEHALF OF CBEC	**FOR AND BEHALF OF** _____
Signature	**Signature**
Name:	**Name:**
Designation:	**Designation:**
Dated :	**Dated:**
Place:	**Place:**
IN THE PRESENCE OF	**IN THE PRESENCE OF**
Signature	**Signature**
Name:	**Name:**
Designation:	**Designation:**
Dated :	**Dated:**
Place:	**Place:**

17. Annex H-Definitions

S.No.	Term	Definition
1	EDW	An Enterprise Data Warehouse (EDW) is a central repository of the business information designed for query and analysis rather than for day-to-day transaction processing. It contains both data from multiple applications and historical data.
2	ISO 27001	ISO 27001 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27.[2] It is a specification for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process
3	IT ACT 2000	Information Technology Act (IT Act) is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. Information Technology Act 2000 addressed the following issues:

		1.Legal recognition of electronic documents 2.Legal Recognition of digital signatures 3.Offenses and contraventions 4.Justice dispensation systems for cybercrimes
4	NDA	NonDisclosureAgreements(NDA)isa confidentiality agreement or contract creating a legal obligation to privacy and compels those who agree to keep any specified information secured or secret.
5	SFTP	Secure File Transfer Protocol (SFTP) is a network protocol that provides file access, file transfer and file management functionalities over any reliable data stream.
6	XML	Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. XML is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere. XML was created to structure, store and transport information. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services.