OECD

BETTER POLICIES FOR BETTER LIVES

Global Forum on Transparency
and Exchange of Information for Tax Purposes

JOINT OECD/GLOBAL FORUM GUIDE ON THE PROTECTION OF CONFIDENTIALITY OF INFORMATION EXCHANGED FOR TAX PURPOSES

GLOBAL FORUM ON TRANSPARENCY AND EXCHANGE OF INFORMATION FOR TAX PURPOSES

The Global Forum on Transparency and Exchange of Information for Tax Purposes is the multilateral framework within which work in the area of tax transparency and exchange of information is carried out by over 110 jurisdictions which participate in the Global Forum on an equal footing.

The Global Forum is charged with in-depth monitoring and peer review of the implementation of the international standards of transparency and exchange of information for tax purposes. These standards are primarily reflected in the 2002 OECD Model Agreement on Exchange of Information on Tax Matters and its commentary, and in Article 26 of the OECD Model Tax Convention on Income and on Capital and its commentary as updated in 2004, which has been incorporated in the UN Model Tax Convention.

The Global Forum Member Countries are Andorra; Anguilla; Antigua and Barbuda; Argentina; Aruba; Australia; Austria; The Bahamas; Bahrain; Barbados; Belgium; Belize; Bermuda; Botswana; Brazil; Brunei Darussalam; Canada; the Cayman Islands; Chile; Colombia; Cook Islands; Costa Rica; Curaçao; Cyprus; the Czech Republic; Denmark; Dominica; El Salvador; Estonia; Finland; France; FYROM; Georgia; Germany; Ghana; Gibraltar; Greece; Grenada; Guatemala; Guernsey; Hong Kong, China; Hungary; Iceland; India; Indonesia; Ireland; Isle of Man; Israel; Italy; Jamaica; Japan; Jersey; Kazakhstan; Kenya; the Republic of Korea; Latvia; Liberia; Liechtenstein; Lithuania; Luxembourg; Macao, China; Malaysia; Malta; Marshall Islands; Mauritania; Mauritius; Mexico; Monaco; Montserrat; Morocco; Nauru; the Netherlands; New Zealand; Nigeria; Niue; Norway; Panama; the People's Republic of China; the Philippines; Poland; Portugal; Qatar; the Russian Federation; Saint Kitts and Nevis; St Lucia; St Vincent and the Grenadines; Samoa; San Marino; Saudi Arabia; the Seychelles; Singapore; Sint Maarten; the Slovak Republic; Slovenia; South Africa; Spain; Sweden; Switzerland; Trinidad and Tobago; Tunisia; Turkey; the Turks and Caicos Islands; the United Arab Emirates; the United Kingdom; the United States; Uruguay; Vanuatu; the Virgin Islands (British); Virgin Islands (USA).

Table of Contents

Introduction

The number of exchange of information agreements has increased dramatically in recent years and in order for jurisdictions to take advantage of the opportunities that this rapidly expanding network provides, jurisdictions and their taxpayers need to have confidence in the confidentiality of the information exchanged under these agreements. Both taxpayers and governments have a legal right to expect that information exchanged under exchange of information agreements remains confidential. This requires that exchange of information partners have adequate safeguards to protect the confidentiality of the information that is shared and assurances that the information provided will only be used for the purposes permitted under the exchange of information instrument.

Confidentiality of taxpayer information has always been a fundamental cornerstone of tax systems. In order to have confidence in their tax system and comply with their obligations under the law, taxpayers need to have confidence that the often sensitive financial information is not disclosed inappropriately, whether intentionally or by accident. Citizens and their governments will only have confidence in international exchange if the information exchanged is used and disclosed only in accordance with the agreement on the basis of which it is exchanged. As in the domestic context, this is a matter of both the legal framework as well as having systems and procedures in place to ensure that the legal framework is respected in practice and that there is no unauthorized disclosure of information. What applies in the domestic context regarding protecting the confidentiality of tax information equally applies in the international context.

Developing the Guide

This guide was developed by the OECD as a tool to help ensure that the requirements to maintain confidentiality under all exchange of information instruments are properly observed. OECD member countries generally have extensive exchange of information networks, including agreements with many non-OECD members. The increase in coverage of the Multilateral Convention on Mutual Assistance has also expanded the universe of jurisdictions involved in exchange of information. As already noted, the

preservation of the confidentiality of information exchanged is crucial to ensuring that these relationships run smoothly.

The Global Forum's standard for confidentiality is based on the 2002 OECD Model Agreement on Exchange of Information on Tax Matters and its commentary, and in Article 26 of the OECD Model Tax Convention on Income and on Capital and its commentary as updated in 2004 and adopted by the OECD Council in 2005. Indeed, Article 26 (Exchange of Information) of the OECD Model Tax Convention is one of the sources of the Global Forum's standards, and all members of the OECD are also members of the Global Forum. In order to ensure that the OECD guide receives the widest possible dissemination, and can benefit both OECD and non-OECD members, the Global Forum is pleased to re-issue it, guaranteeing that it reaches the Global Forum's 110 members. The Global Forum can also promote the guide to non-members through its membership efforts and regional training seminars.

The substance of the guide developed by the OECD is not changed. It has been revised to provide illustrative examples from non-OECD members of the Global Forum, based on information contained in the Global Forum's peer review reports and some of the language has been updated to reflect the Global Forum's more diverse membership.

What's inside

The report sets out the best practices related to confidentiality and provides practical guidance, including recommendations and a checklist, on how to meet an adequate level of protection while recognising that different tax administrations[1] may have different approaches to ensuring that in practice they achieve the level required for the effective protection of confidentiality. Of course, the first step is ensuring that appropriate legislation is in place, but the confidentiality of taxpayer information within a tax administration is not simply the result of legislation. The ability to protect the confidentiality of tax information is also the result of a "culture of care"within a tax administration. This requires that confidentiality measures be incorporated into all the operations of the tax administration. Confidentiality is a cornerstone for all functions carried out within the tax

[1] For most members of the Global Forum exchange of information is carried out by the tax administration. However, in some jurisdictions that do not have direct taxes, the responsibility for exchange of information will be with some other authority, such as the department of finance or a separate authority specifically in charge of handling EOI cases. The reference here to tax administrations should be read to include other types of governmental authorities that may be responsible for exchange of information.

administration and as the sophistication of the tax administration increases, the confidentiality processes and practices must keep pace.

This report provides general guidance on how tax administrations protect the confidentiality of taxpayer information both domestically and also specifically with regard to exchange of information under exchange of information (EOI) instruments. Examples of certain jurisdictions practices are provided to illustrate how some jurisdictions are addressing this very complex subject. Recommendations in Part III provide guidance on the rules and practices that must be in place to ensure the confidentiality of tax information exchanged under exchange of information instruments. For ease of reference the report also contains a checklist.

PART I.

Legal Framework to Protect the Tax Confidentiality of Information Exchanged

1. Tax confidentiality provisions in tax treaties, Tax Information Exchange Agreements (TIEA) and multilateral instruments on mutual administrative assistance

Effective mutual assistance between competent authorities requires that each competent authority be assured that the other will treat with proper confidence the information which it obtains in the course of their co-operation. For this reason all treaties and exchange of information instruments contain provisions regarding tax confidentiality and the obligation to keep information exchanged as secret or confidential. [2]

Information exchange partners may suspend the exchange of information if appropriate safeguards are not in place or if there has been a breach in confidentiality and they are not satisfied that the situation has been appropriately resolved.

Box 1. **Key Points: Tax Confidentiality Provisions in Treaties**

- Confidentiality covers both information provided in a request and information received in response to a request.
- Treaty provisions and domestic laws both apply to ensure confidentiality.
- Information exchanged may only be used for certain specified purposes.
- Information exchanged may only be disclosed to certain specified persons.

2 The complete text of the confidentiality provisions of the TIEA and the multilateral Convention on Mutual Administrative Assistance in Tax Matters can be found in Annex A.

1.1 Confidentiality under Article 26 of the OECD Model Tax Convention

Article 26(2) of the OECD Model Tax Convention provides that:

> *Any information received under paragraph 1 by a Contracting State shall be treated as secret in the same manner as information obtained under the domestic laws of that State and shall be disclosed only to persons or authorities (including courts and administrative bodies) concerned with the assessment or collection of, the enforcement or prosecution in respect of, the determination of appeals in relation to the taxes referred to in paragraph 1, or the oversight of the above. Such persons or authorities shall use the information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions*

This provision states that information received under the provisions of a tax treaty shall be treated as secret in the same manner as information obtained under the domestic laws of the receiving State. Article 26 goes on to provide the confidentiality rules under the Model Convention, the purposes for which the information may be used and limits to whom the information may be disclosed.

Disclosure is limited to persons or authorities (including courts and administrative bodies) involved in the:

- assessment;
- collection;
- enforcement;
- prosecution; and
- determination of appeals

in relation to the taxes with respect to which information may be exchanged under the treaty.

Information may also be communicated to the taxpayer, his proxy or to a witness. Information can be disclosed to governmental or judicial authorities charged with deciding whether such information should be released to the taxpayer, his proxy or to the witnesses. The information shall only be used for the above purposes. Courts and administrative bodies involved in the tax purposes discussed in paragraph 9 can disclose the information in court sessions or court decisions, once information becomes

public in this way, that information can then be used for other purposes.[3] The confidentiality rules cover competent authority letters, including the letter requesting information. It is understood that the requested state can disclose the minimum information contained in a competent authority letter (but not the letter itself) necessary for the requested state to be able to obtain or provide the requested information to the requesting state, without frustrating the efforts of the requesting state.

Information may also be disclosed to oversight bodies.

Information may not be disclosed to a third country unless there is an express provision in the bilateral treaty allowing it. It may not be used for other (non-tax) purposes unless otherwise specified in the treaty. In this respect countries may include a provision which allows the sharing of information with other law enforcement agencies when such information may be used for such other purposes under the laws of both countries and the competent authority of the supplying countries authorises such use.

The provisions of Article 26(2) concern information exchanged under Article 26 and also apply to information exchanged relating to the Mutual Assistance Procedure and Assistance in Tax Collection.

1.2 Confidentiality under Article 8 of the Model Agreement on Exchange of Information on Tax Matters ("TIEA")

Article 8 of the TIEA provides that:

> *Any information received by a Contracting Party under this Agreement shall be treated as confidential and may be disclosed only to persons or authorities (including courts and administrative bodies) in the jurisdiction of the Contracting Party concerned with the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, the taxes covered by this Agreement. Such persons or authorities shall use such information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions. The information may not be disclosed to any other person or entity or authority or any other jurisdiction without the express written consent of the competent authority of the requested Party.*

The TIEA is similar to the Model Convention as they both require that information be kept confidential and limit the persons to whom the information can be disclosed and the purposes for which the information

3 Paragraphs 12-13 of the Commentary to Article 26 of the Model Convention.

may be used. The Model Convention contains the additional requirement that information should be treated "as secret in the same manner as information obtained under domestic law." However, because both the TIEA and the Model Convention specify to whom the information can be disclosed and for what purposes the information may be used (thus ensuring a minimum standard of confidentiality), there should be little practical difference between the two formulations.[4] There are also some differences. First, the Model Convention also permits disclosure to oversight authorities[5]. Second, the TIEA expressly permits disclosure to any other person, entity, authority or jurisdiction provided express written consent is given by the competent authority of the requested party.[6]

1.3 Confidentiality under Article 22 of the multilateral Convention on Mutual Administrative Assistance in Tax Matters

The Multilateral Convention states:

Article 22 – Secrecy

1. Any information obtained by a Party under this Convention shall be treated as secret and protected in the same manner as information obtained under the domestic law of that Party and, to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Party as required under its domestic law.

2. Such information shall in any case be disclosed only to persons or authorities (including courts and administrative or supervisory bodies) concerned with the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, taxes of that Party, or the oversight of the above. Only the persons or authorities mentioned above may use the information and then only for such purposes. They may,

4 See paragraph 57 of the Manual on the Implementation on Exchange of Information Provisions for Tax Purposes, Module on General and Legal Aspects of Exchange of Information.

5 Oversight authorities are authorities that supervise the tax administration and enforcement authorities as part of the general administration of the government of the contracting parties (see paragraphs 12 and 12.1. of the Commentary to Article 26 of the Model Convention).

6 The Global Forum standards refer to the OECD Model Tax Convention as updated in 2004. In July 2012, article 26 (2) of the OECD Model Tax Convention was updated to include the following provision: Notwithstanding the foregoing, information received by a Contracting State may be used for other purposes when such information may be used for such other purposes under the laws of both States and the competent authority of the supplying State authorises such use.

notwithstanding the provisions of paragraph 1, disclose it in public court proceedings or in judicial decisions relating to such taxes.

The Multilateral Convention is similar to both the Model Convention and the TIEA as all three require that the information be kept confidential and similar to the Model Convention it makes a specific reference to domestic law. Both the Model Convention and the Multilateral Convention allow disclosure to supervisory bodies. Further, similar to the TIEA, the Multilateral Convention permits the information to be used for other purposes where such other use is authorised by the requested party. The Multilateral Convention differs in that it makes specific reference to the protection of personal data. However, as all of the instruments specify that information must be kept confidential, can only be disclosed to certain persons and used for certain purposes, this should result in little practical difference.

2. Tax confidentiality provisions in domestic legislation

Jurisdictions usually have domestic legislation to ensure confidentiality of tax information, including information exchanged. These rules can be found in domestic tax legislation provisions which restrict government officials (and sometimes others) from disclosing information except in certain circumstances, from broader rules that apply to all civil servants (not only those working in the field of taxation), or in specialised legislation governing exchange of information for tax purposes. As part of its peer review process, the Global Forum examines the adequacy of confidentiality provisions both in a jurisdiction's exchange of information agreements and its domestic laws. The peer review reports are available on the Global Forum's EOI Portal at www.eoi-tax.org.

Box 2. **Key Points: Tax Confidentiality Provisions in Domestic Laws**

- Domestic laws must be in place to protect confidentiality of tax information.
- Treaty obligations regarding confidentiality must be binding in countries.
- Effective penalties must be in place for unauthorised disclosures of confidential information exchanged.

Jurisdictions implement their treaty obligations (including confidentiality obligations) in different ways. One approach is to amend

domestic legislation to ensure that all treaty obligations are respected under domestic law. This requires a review of domestic legislation to ensure that the treaty obligations are met and to amend domestic law if necessary. In other jurisdictions, obligations under tax treaties are implemented in such a way that in the event of an inconsistency between a treaty and domestic law, the treaty overrides the domestic law. Some countries use a combination of the two approaches.

Box 3. **Illustrative examples**

In the United Kingdom when there are inconsistencies between domestic law and treaties, the legislation introducing treaties into domestic law makes it clear that the treaty takes precedence.

In Barbados, treaties have the force of law notwithstanding anything in any other enactment and their terms therefore prevail over the domestic tax legislation.

In Brazil, the Supreme Federal Court recognises that international agreements override domestic tax legislation, including ordinary laws enacted later in time.

In Denmark and Sweden there is legislation providing that any restrictions imposed by the requested state on the use of received information shall apply even if contrary to their domestic law.

In the United States, if confidentiality requirements under domestic law are more restrictive than the confidentiality requirements under an international agreement, the more restrictive domestic law requirement is used.

Regardless of the approach adopted, jurisdictions must ensure that the confidentiality obligations are respected when information is received under a tax treaty or other exchange of information mechanism.

Other domestic laws must also be reviewed to ensure that they do not require or allow the release of information obtained under a tax treaty or other exchange of information instrument. For example, information may not be disclosed to persons or authorities not covered in Article 26 regardless of domestic information disclosure laws (for example freedom of information or other legislation that allows access to governmental documents). Many jurisdictions have specific exemptions in their freedom of information laws so that information obtained under tax treaties is not subject to disclosure.

Box 4. **Illustrative example**

In Canada, Section 13 of the Access to Information Act and Section 19 of the Privacy Act specifically provide that information received in confidence from a foreign government cannot be disclosed unless the foreign government consents to the disclosure.

Finally, domestic legislation must set out penalties for persons or authorities who improperly disclose confidential information. Both administrative penalties and criminal penalties may apply. In many jurisdictions the penalties are contained in the domestic legislation dealing with taxation in other countries the penalties are contained in other domestic legislation, such as the penal code. Penalties must be clear and severe enough to discourage breaches.

Box 5. **Illustrative Examples**

In Anguilla, the sanction for contravention of the confidentiality provisions are a fine of USD 3703 or imprisonment for up to 2 years or both on summary of conviction.

In France, the penalty for the disclosure of secret information is punishable by one year's imprisonment and a fine of up to EUR 15 000 under the Penal Code.

In Germany, public officials who breach tax secrecy can be punished by imprisonment of up to two years or by a fine.

In Malta, any person in breach of confidentiality is guilty of an offence and on conviction, liable to a fine from EUR 232 to EUR 2325 or to imprisonment for up to 6 months or both.

In Poland, revealing secret information is punishable by deprivation of liberty from six months to five years.

In the United Kingdom, disclosure provisions can result in a penalty of up to two years' imprisonment and an unlimited fine.

In New Zealand, legislation allows for up to six months imprisonment, a fine of NZD 15 000 or both.

In the Philippines, employees breaking the duty of confidentiality are punishable with a fine of PHP 50 000 to 100 000 (USD 1 100 to 2 200) and/or imprisonment for two to five years.

In Italy, a public officer that is responsible for an unauthorized disclosure of confidential information is subject to imprisonment for six months to three years, if that officer has illegally accessed confidential databases he is subject to one to

five years imprisonment.

PART II.

Administrative Policies and Practices to Protect Confidentiality

1. Introduction

As a result of the obligation to protect confidentiality, jurisdictions have developed domestic policies and practices to effectively implement their treaty and domestic law obligations. Many of these policies and practices were developed to ensure confidentiality for domestic tax purposes but they are also useful for protecting information that has been exchanged under tax treaties. Jurisdictions have also developed certain practices specifically for protecting the confidentiality of information exchanged under tax treaties and other exchange of information mechanisms.

Box 6. **Key Points: Administrative Policies and Practices to Protect Confidentiality**

- A comprehensive policy to ensure the confidentiality of tax information must be in place.
- The comprehensive policy must be reviewed and endorsed at the top level.
- The tax administrationmust designate a person or persons to be responsible for implementing the policy.
- The comprehensive policy must include:
  - background checks/security screening of employees;
  - employment contracts;
  - training;
  - access to premises;
  - access to electronic and physical records;
  - departure policies;
  - information disposal policies; and
  - managing unauthorised disclosures.
- Information sent to a foreign competent authority must be transmitted securely and in the case of electronic transmission, with an appropriate level of encryption.
- Information and incoming requests received from a foreign competent authority must be appropriately classified, securely stored and steps taken to ensure its use and disclosure are in compliance with the treaty or information exchange mechanism.

2. Comprehensive policy and procedures in place, reviewed and approved at top level

Effectively protecting the confidentiality of information and in particular any personal information is a key concern for tax administrations. It is therefore necessary for tax administrations to develop a comprehensive policy including procedures to ensure that the legal framework is effectively implemented. Such policy and procedures need to be reviewed and endorsed at the top level of a tax administration. Further, it needs to be clarified who in the organisation is responsible for implementing the policy. As discussed in more detail below, the comprehensive policy should cover all aspects relevant to protecting confidentiality and include background/security checks of employees, employment contracts, training, access to premises, access to electronic and physical records, departure policies, information disposal policies and managing unauthorized disclosures of confidential

information. In addition to having a comprehensive policy in place, tax administrations must regularly monitor compliance with the policy in practice. For example, spot checks can be an effective means to ensure that unauthorized individuals cannot access the premises and physical records are locked in a cabinet or otherwise securely stored.

2.1. Individual Aspects to Protecting Confidentiality

Employees (background checks, employment contracts, training): Steps should be taken to ensure that employees are required to undergo an appropriate level of background checks/security screening to help ensure that they will be responsible employees and not represent a security risk. The employment contract should contain provisions dealing with the employee's obligations with respect to confidentiality of tax information and describe the sanctions if the obligations are breached. The obligation to maintain tax secrecy should continue after the end of the employment relationship. Consultants, service providers, contractors and others having access to confidential tax information should also be subject to background checks/security screening and be contractually bound by the same obligations as employees with respect to confidentiality of tax information.

Box 7. **Illustrative Examples**

In Denmark and Slovenia all tax administration employees must sign a statement of confidentiality when employed.

In Japan, Article 100 of the National Public Service Act states that national public officers shall not disclose information which is obtained through their work and this also applies after their retirement.

In Jersey, all officers of the Competent Authority Office are required to swear an oath before the Royal Court in respect of their duties, which include confidentiality.

In Mauritius, each officer of the Mauritius Revenue Agency is required to take an oath of secrecy before starting to perform his/her duties.

Furthermore, domestic legislation must contain sanctions in circumstances where employees breach confidentiality obligations (see Part I). Employers have a duty to inform employees of their responsibility to protect confidentiality and provide training on this issue so that employees have a proper understanding of their obligations, as well as the procedures and processes in place to protect confidentiality. All employees and others having access to confidential tax information must be provided adequate training, especially competent authority staff and auditors who use the

information exchanged. Employers should also ensure that employees are periodically reminded of their obligations and training is provided regularly to reinforce the obligations and procedures, and process in place to protect confidentiality. Employees should also be trained to report actual or potential breaches of confidentiality.

Access to Premises: Tax administrations must restrict entry to their buildings/premises for security reasons, including the protection of confidential tax information. Measures often include the presence of security guards, policies against unaccompanied visitors, security passes or coded entry systems for employees and also limiting access by employees to areas where sensitive information is located. Some administrations, such as Australia, also have clear desk policies to ensure that confidential information is locked away when not being used (when employees are away from their desks and overnight).

Access to Electronic and Physical Records: Tax administrations must provide secure storage for confidential documents. The level of security may depend on the security classification of the information. Information can be secured in locked storage units or rooms. This includes cabinets (whether locked with combinations or keys), safes and strong rooms. There should be a policy that limits who has access to combinations and keys. The security of the physical storage cabinets vary depending on the classification of the material.

Tax administrations must also ensure that confidential tax information is kept on secure servers and firewalled (*i.e.* cannot be accessed by unauthorized persons) and password protected (cannot be accessed without a password). Each employee should have a unique user id and password and there should be a record of who has accessed specific information. This also helps to limit employee access to non-essential information. Access to databases containing confidential information is limited to employees who need to use it. Many jurisdictions have internal systems and audit systems in place to ensure that confidentiality policies are being respected.

Box 8. **Illustrative Examples**

In Italy, any tax official making a query on the tax database must acknowledge their legal obligations and all operations are recorded and monitored. Italy has an Internal Audit Service at the central and local level, this group works with the Privacy Guarantor in order to monitor the application of the rules regarding the protection of tax information and to supervise that the security systems are correctly implemented.

In the United States, the IT system has software to review access to taxpayer information; the system is set up to trigger warnings and to identify employees who may be accessing information on neighbours, friends or celebrities. There is then a review process in place to ensure that those files were accessed for legitimate reasons.

In Argentina, to protect the confidentiality of the tax database, each tax official has his/her own "tax key" that he/she must enter for any search or modification to the database. Not all the tax officials have the same level of access to the tax databases, from level 1 to level 4, depending on the responsibilities of the agent. When an agent does not have sufficient access rights, he/she must request access through his/her director. All accesses are tracked and in the case of any unusual access to the tax database, internal auditors question the supervisor of the agent involved.

Tax administrations should also develop policies for all portable equipment including laptops, memory sticks, smart phones and cell phones. For instance, all portable equipment should be password protected or secured in other ways. Due to security concerns some tax administrations do not allow employers to access secure systems with personal devices.

Box 9. **Illustrative Example**

The United Kingdom has a policy such that employees are not permitted to use transferable media without the permission of a specific data guardian in each Directorate. In addition, UK employees cannot travel outside the UK with their work related laptops without the permission of the data guardian.

Departure Policies: Procedures must exist for quickly terminating access to confidential information for employees who leave or who no longer need access to the information to ensure confidentiality of information. These processes can include exit interviews to ensure the employee returns property that allows access to taxpayer information

(*e.g.* laptops, media, keys, identification cards, and building passes). One method is to assign access to specific areas and software based on roles rather than individuals. In that way, if an employee is reassigned from one job to another, the access automatically changes without anyone having to revoke one set of access and start another.

Information Disposal Policies: Tax administrations must have policies regarding secure disposal of confidential information. Most include policies under which confidential information is treated differently than non-confidential information and often disposal procedures vary depending on the level of confidentiality. Shredding documents is commonly used by tax administrations. Disposal can include using burn boxes or depositing confidential information into locked waste bins which are then shredded before information is disposed of. Electronic documents should also be deleted when no longer necessary. Appropriate steps must be taken to remove confidential information when computers and information storage devices are disposed of.

Managing Unauthorized Disclosures of Confidential Information: Policies and procedures must be in place for managing unauthorized disclosures of confidential information.

Box 10. **Key Points:**
Managing Unauthorized Disclosures of Confidential Information

- A policy must be in place to manage unauthorized disclosures.
- Once an unauthorized disclosure occurs, there must be an investigation followed by the preparation of a report for management.
- The report must include:
    - recommendations for minimising the repercussions of the incident;
    - an analysis of what should be done in the future to avoid similar incidents; and
    - recommendations for any actions/penalties to be taken against the person or persons responsible for the breach, noting that law enforcement authorities may be involved in the case of suspected intentional disclosure.
- The recommendations must lead to a high degree of confidence that the changes once implemented will ensure that a similar breach will not occur in the future.
- The investigating authority or senior management must be responsible to ensure that recommendations are implemented.

As stated above in the paragraph on employees, training should be provided to employees regarding reporting actual or potential breaches of confidentiality. The tax administration also needs to designate a person or group that co-ordinates confidentiality issues and often the administration's security department is in charge of receiving reports of unauthorized disclosure. Once there has been an unauthorized disclosure, there must be an investigation of the incident. The investigation must be broad enough to determine the circumstances that led to the unauthorized disclosure, the person or persons responsible and, where possible, the cause of the breach. The investigation should not hold up any immediate steps that can be taken to minimise the impact.

Following the investigation, a report must be prepared for management and must include:

a) recommendations for minimising the repercussions of the incident;

b) an analysis of what should be done in the future to avoid similar incidents; and

c) recommendations for any actions/penalties to be taken against the person or persons responsible for the breach, noting that law enforcement authorities may be involved in the case of suspected intentional disclosure.

It is also necessary for the investigating authority or senior management to be responsible for following up to ensure that recommendations are implemented by the tax administration . The recommendations in the report should result in ensuring a high degree of confidence that the changes once implemented will ensure that a similar breach will not occur in the future. Jurisdictions need to ensure that penalties are imposed when breaches in confidentiality actually occur and deficiencies in procedures and processes are identified and immediately addressed and rectified.

When taxpayer confidentiality is violated, it may be the result of an unintentional act, deficiencies in the systems and procedures to protect the confidentiality of tax information or in other cases it may be the result of intentional actions, for the personal gain of one or more persons (for example because of corruption). Whether the breach is the result of intentional or unintentional actions any breach of confidentiality must be taken seriously and acted upon immediately. The appropriate actions to be taken will vary from situation to situation and depend on the circumstances of the breach. If the breach is the result of an intentional action for personal gain it would generally be appropriate to refer such matter to law enforcement officials for possible criminal charges.

Box 11. **Illustrative Example**

In Ireland, trained investigators are granted access to all the necessary information to investigate and they report their findings to senior management. Human Resources Management makes the determination on the resulting action which can result in dismissal and/or referral to law enforcement officials for possible criminal charges.

3. Practices adopted by tax administrations to protect the tax confidentiality of information during the transmission of information exchanged under a tax treaty or other exchange of information instrument

The confidentiality of information that has been exchanged must be ensured throughout the various stages of the exchange of information process. This section addresses precautions that can be taken when the information is transmitted to a foreign tax authority. Information includes

the requests themselves, related correspondence and the information exchanged pursuant to the request.

3.1 Sending information to a foreign tax authority

Prior to sending information many competent authorities have procedures/processes in place to ensure that the information they send will be kept confidential. This includes confirming that the person who has requested the information was authorized to make the request and to receive the information. Steps should be taken to confirm that the competent authority name and address are correct before sending any information. All confidential information should be clearly labelled.

In order to ensure the tax confidentiality of information exchanged, the competent authorities of a number of jurisdictions include an embedded warning in the competent authority letter and all enclosures (background information, copies of contracts, etc.) such as a treaty stamp for paper mail or a watermark in case of electronic exchange. Such treaty stamp or watermark often states:

> THIS INFORMATION IS FURNISHED UNDER THE PROVISIONS OF A TAX TREATY AND ITS USE AND DISCLOSURE ARE GOVERNED BY THE PROVISIONS OF SUCH TAX TREATY.

These types of warnings are also placed on documents that the receiving competent authority forwards to other officers within the tax administration (*e.g.* auditors). This is discussed below in the section on sending information within the tax administration.

Physical mail should only be sent via an international registration system where a mail tracking function is in place. The mail received from foreign competent authorities should be delivered directly to the EOI Unit and stored in secure cabinets (see section on Storage below).

Information sent electronically must remain confidential during transmission from the sender's computer system to the recipient's computer system. Confidentiality before and during transmission is the responsibility of the sending authority. After receipt it is the responsibility of the receiving authority. Only persons authorized to receive information under the treaty should be able to access the mailboxes of the competent authorities.

In some cases, the competent authorities can exchange information using a secure platform. In other cases, letters and taxpayer information are sent in encrypted files attached to email messages. Tax administrations must ensure that the information exchanged is transmitted securely, with an appropriate level of encryption.

3.2 Transmission for automatic exchange

With respect to automatic exchange of information, records should be transmitted by encrypted CDs **(**or an alternative secure format), secure platform, or encrypted files attached to e-mail messages. In the experience of some countries, large files may need to be broken down into smaller files as many countries do not have the capacity to receive more than 5MB per transmission.

4. Practices adopted by tax administrations to ensure the confidentiality of information that has been received from a treaty partner

This section addresses precautions that can be taken when the information is received, used and stored. Many countries have specific administrative guidelines with respect to the confidentiality of information received under EOI.

4.1 Classification of information received from a foreign competent authority

Classification: Most domestic confidentiality systems require information to be classified according to its level of confidentiality/secrecy. Information received from a foreign tax authority must be suitably classified to ensure that it remains confidential and the restriction on its use and disclosure are respected.

4.2 Storage of and access to information received from a foreign competent authority

Storage: Information obtained from other competent authorities must be securely stored. In some cases it is entered into a database that is separate from the normal tax administration database.

Box 12. **Illustrative Example**

In Ireland, information received from other competent authorities is stored in its own database which can be accessed only by staff in the competent authority office. CDs received from other countries are stored in secure cabinets with combination locks.

In South Africa, all documents pertaining to a request for information received from another jurisdiction are scanned and stored on a secure server. Only the personnel directly involved in exchange of information cases has access to this server.

In other cases, jurisdictions may not use stand alone databases but put the information received on the main system of the tax administration but then limit access to the information.

Access to information exchanged: Whether the information is stored on a separate database or the main tax administration system, all incoming requests for information and all information received should be entered into an internal IT management system to which only authorised officials have access by individual login and password. Access should be strictly controlled based on a need to know principle and could be by express permission only. These internal systems should leave an electronic fingerprint that allows identification of the officials who are accessing the files. Stand alone systems for EOI that are not connected to the main network also restrict electronic access.

Box 13. **Illustrative Examples**

In Australia, ATO field staff record the material on the ATO computer system, but can restrict access to the electronic information so that only immediate team members and the EOI Unit have access. This ensures that no inappropriate dissemination occurs (such as income tax related material being used for GST/VAT purposes as some of Australia's older treaties do not permit that to occur).

In Denmark, information received through automatic exchange in Denmark is registered and saved in computer files which only three persons from the competent authority have access to. These employees sort the information and forward only what is necessary to the assessors.

In Germany, only staff members who are entitled to view the data relating to exchanges of information are able to do so. This occurs via special access rights granted on separate IT systems for each individual and subsequent approval by the head of division. In addition, all information is kept electronically. The German authorities have implemented an IT system dedicated to EOI to store all requests in an electronic format and facilitate transmissions to local authorities by e-mail.

No hard copies of requests are kept. Regional and local authorities in Germany do not have access to the IT system for exchange of information.

In the Isle of Man, all correspondence received and responses made in relation to an EOI request are held electronically by the competent authority and inaccessible to staff other than those involved in EOI matters. Hard copies are held on separate EOI files which are regularly scanned into a secure area. No copies of EOI material are held on the tax files of persons who have been the subject of an EOI request.

Hard copies of incoming information should only be made if necessary. Hard copies should be kept securely by the official to whom the case is allocated. Information should be kept in secure locked filing cabinets or strong rooms and access restricted as necessary. Hard copies should be disposed of in a secure manner when no longer necessary. For instance, in Portugal only one employee has access to the paper archive and that person controls access to needed files or documents.

Depending on the domestic classification system, exchange of information officers may need a higher level of classification than some other employees. IT staff involved with EOI databases and other IT matters that have access to confidential treaty information also need appropriate security checks and training to ensure that confidentiality is not breached.

4.3 Transmission of information from the competent authority to other areas of the tax administration

Precautions taken by competent authorities: It is often necessary for information to be sent by the competent authority to other officials or authorities within the tax administration or justice department. A record should be kept showing who the information has been disclosed to, how many copies have been produced and who has a copy in their possession at any time. In many cases, the competent authority receives large amounts of information regarding many taxpayers, often only a portion of that information is required by a specific auditor in a certain region of the country. Competent authority staff are responsible for ensuring that only the specific information needed by the particular individuals is forwarded and that bulk information is not simply retransmitted.

As discussed above, treaty stamps and warnings are often used to protect confidentiality of the information when sent by one competent authority to another. Competent authorities who then forward that information within the tax administration also include warnings. In addition to stating that the information is confidential and has been obtained under a tax treaty, some of these warnings may advise that the information may not be disclosed under

freedom of information laws or without consulting the competent authority in advance. This is done to help ensure that unauthorized disclosure does not occur.

Box 14. **Illustrative Example**

In Canada, the Canadian Competent Authority attaches the following warning to documents sent to their field offices:

> All information received under the exchange of information provisions of a treaty may only be used for tax purposes and must be maintained in the strictest confidence. Release of these documents, either informally or under the Access to Information Act or the Privacy Act, must be discussed with Exchange of Information Services prior to disclosure. Section 1.11 of the Exchange of Information Reference Guide, located on the Infozone[7], provides further details.

Some jurisdictions include warnings on the cover page and other jurisdictions include the warning on each page of the information in case pages become separated.

Where the exchange of information mechanism allows the information to be used for other (non-tax) purposes, the receiving law enforcement agencies and judicial authorities must treat that information as confidential consistent with the exchange instrument.

7 An internal tax administration website.

Box 15. **Illustrative Examples**

In the United Kingdom, when the competent authority forwards information to auditors, the information is treaty stamped. When information is sent by CD, the treaty stamp is also placed on the CD.

In Australia, when information is communicated to tax officials outside the EOI Unit a cover sheet is attached to the information (see Annex B for a copy of the cover sheet). It clearly states that the information must not be passed on or copied without the prior consent of the EOI Unit. This cover sheet also directs readers to two ATO Practice Statements. One practice statement covers limitations on the use of the material in regard to older tax treaties that do not cover indirect taxes. The other explains what to do if the information is requested as part of a Freedom of Information request.

In Slovenia, documents include a warning that persons obtaining confidential tax information:

- may use the information only for the purpose for which it was provided,
- may not disclose to third parties any confidential tax information previously disclosed to them,
- shall ensure the same measures and procedures for the protection of confidential tax information as specified for the tax authority.

PART III.

Recommendations

The following recommendations are designed to help tax administrations ensure that confidential taxpayer information is being adequately safeguarded. In principle these recommendations and best practices are designed for information exchanged but are also equally applicable to the treatment of tax information obtained and used domestically.

I. Legal Framework

1. Jurisdictions should ensure that instruments that allow exchange of tax information expressly require the confidentiality of such information be maintained.

2. Jurisdictions must have legislation in place to ensure that information exchanged under a tax treaty or other exchange of information mechanism will be kept confidential in accordance with their treaty obligations.

3. Domestic legislation (for example, freedom of information or access to information) must not require or allow the release of information obtained under a tax treaty or other exchange of information mechanism in a manner inconsistent with the confidentiality obligations in that mechanism.

4. There must be sufficient sanctions in place when confidentiality obligations have been breached to deter such behaviour. These need to be made known, be strong enough to have a deterrent effect and ensure that breaches will be dealt with effectively.

II. Administrative Policies and Practices to Protect Confidentiality

5. Comprehensive policies and procedures on confidentiality of tax information must be in place, reviewed regularly and endorsed at the

top level of a tax administration. Further, it must be clear who within the administration is responsible for implementing the policy.

6. Background checks/security screening must be conducted for all persons that will have access to confidential information.

7. The employment contract/arrangement must contain provisions dealing with the employee's obligations with respect to confidentiality of tax information and such obligations should continue post employment. Consultants, service providers and contractors must be contractually bound by the same obligations as employees (whether fulltime or temporary) and these obligations should continue to prevail beyond the period of the contract or engagement.

8. Employers must provide training and reminders on a regular basis which explain the employee's responsibilities with respect to confidential tax information including a clear understanding of where they can obtain assistance if they have questions or require advice.

9. Premises, or areas within those premises, which contain confidential tax information must be secure and not accessible by unauthorized persons.

10. When documents containing confidential information (whether paper or electronic) are stored, circulated, accessed or disposed of, this must be done in a secure manner to ensure the confidentiality of the documents is maintained.

11. Policies and procedures must be in place for managing unauthorized disclosures of confidential information. If an unauthorised disclosure takes place an investigation must be undertaken and a complete report including recommendations must be prepared. The recommendations in the report should result in ensuring a high degree of confidence that the changes, once implemented, will ensure that a similar breach will not occur in the future. Sanctions provided for in domestic law must be applied against the person or persons responsible in a manner that will deter breaches from occurring in the future.

12. Tax administrations must ensure that information sent by a competent authority electronically or by mail is transmitted securely and in the case of electronic transmission with an appropriate level of encryption. Where CD ROMs are used, they must be encrypted.

13. All incoming requests for information and all information received must be stored in a secure manner. Access should be strictly controlled and

on a need to know basis. Where an IT system is used, access should be by individual login and password. A system which leaves an electronic fingerprint that allows identification of the officials who are accessing the files is desirable. When information is stored in paper format it must be placed in a locked cabinet with restricted access.

14. Competent authorities must take precautions when storing or sending EOI information to others within the tax administration. Only necessary information should be sent and it should be clearly identified as information received from a treaty partner, noting that there are restrictions on its use and disclosure.

PART IV.

Checklist

	Checkpoints	Yes	No
1	Treaty or other exchange of information mechanism is in place and provides for the confidentiality of tax information.		
2	Domestic legislation is in place to adequately protect the confidentiality of tax information.		
3	Domestic legislation includes sufficient sanctions for breaches of confidentiality.		
4	A comprehensive policy on confidentiality of tax information is in place and endorsed at the top level of the administration.		
5	A specified person is responsible for implementing the comprehensive policy.		
6	The comprehensive policy includes:		
	(a) background checks/ security screening of employees,		
	(b) employment contracts,		
	(c) training,		
	(d) access to premises,		
	(e) access to electronic and physical records,		
	(f) departure policies, and		
	(g) information disposal policies, and		
	(h) managing unauthorized disclosures.		
7	All aspects of the policy have been implemented in practice.		

	Checkpoints	Yes	No
8	Have any breaches in confidentiality occurred?		
	If yes, (a) was the breach investigated?		
	(b) was a report with recommendations prepared?		
	(c) did the recommendations in the report result in a high degree of confidence that the changes, once implemented, would ensure that a similar breach would not occur?		
	(d) were the recommendations effectively implemented?		
	(e) were the sanctions provided for in domestic law applied to the person or persons responsible in a manner that will deter future breaches?		

ANNEX A.

Confidentiality Provisions in Exchange of Information Instruments

Model Agreement on Exchange of Information on Tax Matters

Article 8

Any information received by a Contracting Party under the Agreement shall be treated as confidential and may be disclosed only to persons or authorities (including courts and administrative bodies) in the jurisdiction of the Contracting Party concerned with the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, the taxes covered by this Agreement. Such persons or authorities shall use such information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions. The information may not be disclosed to any other person or entity or authority or any other jurisdiction without the express written consent of the competent authority of the requested Party.

The Multilateral Convention on Mutual Administrative Assistance in Tax Matters as amended by the 2010 Protocol

Article 22 – Secrecy

1. Any information obtained by a Party under this Convention shall be treated as secret and protected in the same manner as information obtained under the domestic law of that Party and, to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Party as required under its domestic law.

2. Such information shall in any case be disclosed only to persons or authorities (including courts and administrative or supervisory bodies) concerned with the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, taxes of that Party, or the oversight of the above. Only the persons or authorities

mentioned above may use the information and then only for such purposes. They may, notwithstanding the provisions of paragraph 1, disclose it in public court proceedings or in judicial decisions relating to such taxes.

3. If a Party has made a reservation provided for in sub-paragraph a. of paragraph 1 of Article 30, any other Party obtaining information from that Party shall not use it for the purpose of a tax in a category subject to the reservation. Similarly, the Party making such a reservation shall not use information obtained under this Convention for the purpose of a tax in a category subject to the reservation.

4. Notwithstanding the provisions of paragraphs 1, 2 and 3, information received by a Party may be used for other purposes when such information may be used for such other purposes under the laws of the supplying Party and the competent authority of that Party authorizes such use. Information provided by a Party to another Party may be transmitted by the latter to a third Party, subject to prior authorisation by the competent authority of the first-mentioned Party.

ANNEX B.

Country Example

NOTICE	ATO STAFF		IN CONFIDENCE
FORMAT	AUDIENCE	DATE	CLASSIFICATION

Australian Government
Australian Taxation Office

You are viewing a document received by the ATO under one of Australia's tax treaties. Special handling procedures apply to such documents.

You must not pass or copy any material exchanged via Australia's tax treaties to external parties without the prior consent of the Exchange of Information (EOI) Unit.

There are also limitations on the use of this material, especially in regard to many of Australia's older tax treaties (for example, use by GST staff of information exchanged for income tax purposes only). Consult PSLA 2007/13.

You must also immediately notify the EOI Unit in National Office if you are asked to provide any of this material as part of any FOI request. Consult PSLA 2006/09.

If you have concerns about the proper use of this material, please contact the EOI Unit via email at AustralianCompetentAuthority@ato.gov.au.