Tax Administration: Privacy, Disclosure and Fraud Risks Related to COVID-19

Version 26 May 2020

OECD

BETTER POLICIES FOR BETTER LIVES

Tax Administration: Privacy, Disclosure and Fraud Risks Related to COVID-19

Version 26 May 2020

Tax administrations around the globe are taking a series of extraordinary measures to support taxpayers and the wider economy, including through helping to deliver wider government support, while also taking a range of actions to ensure continuity of critical operations and the safety of staff and customers. The speed with which those measures are implemented and the adjustments to some tax administration processes and ways of working can lead, however, to a significant increase of the risks of lapses or deviations from disclosure and privacy requirements as well as the risks of fraud.

This document captures some of those high-level risks as well as possible mitigation strategies with a particular focus on remote working issues. It has been produced by the OECD Forum on Tax Administration (FTA) Secretariat in collaboration with the FTA Enterprise Risk Management Community of Interest. It also takes account of input provided by tax administrations, including through virtual meetings, surveys and bilateral discussions. This document does not make recommendations as regards particular measures since national circumstances and considerations will vary greatly. Tax administrations are invited to provide comments on this document by emailing the FTA Secretariat at FTA@oecd.org.

Table of contents

1 Introduction 4

2 Privacy and disclosure risks 5

Office closure and remote working related risks 5
IT related risks 8
Human resource related risks 10

3 Fraud risks 12

Identity fraud risks 12
Tax fraud risks 13
Internal fraud risks 14

1 Introduction

1. During the current period, the risks of lapses or deviations from disclosure and privacy requirements as well as the risks of fraud have increased markedly. This is due to the large increase in remote working, the fast-moving and potentially confusing nature of changes in processes, increased security risks and greater opportunities for errors, misconduct and fraud.

2. This document captures some high-level risks, mitigations, and exposures / vulnerabilities identified by tax administrations that participate in the OECD Forum on Tax Administration's Community of Interest on Enterprise Risk Management. The items included are intended to be input for consideration and discussion and are not intended to be comprehensive.

2 Privacy and disclosure risks

3. Privacy and disclosure risks refer to the probability of the tax administration losing control of tax information, personally identifiable information (PII), or other sensitive information. The loss of control of such information, including potential public disclosure, can have adverse consequences for the public trust in the wider tax system, with implications for overall tax compliance, and can potentially cause severe reputational damage to the tax administration. The risks included in this chapter, as well as potential mitigation strategies, are categorised as follows:

- ***Office closure and remote working related risks*** – the privacy and disclosure risks related to the closure of tax administration offices and the significant increase in remote working arrangements;
- ***IT related risks*** – the privacy and disclosure risks arising from working on networks that may be less secure than those used in office locations; and
- ***Human resource related risks*** – the privacy and disclosure risks related to the administration's human resource function in the COVID-19 environment.

Office closure and remote working related risks

Unauthorised access to administration offices

4. Administrations are always concerned about break-ins and the theft of information and therefore protect office buildings with a variety of security measures, including requirements for documents and sensitive material to be securely locked away or otherwise protected. While break-ins and theft may typically be a night-time issue, it now also becomes a greater day-time risk in a period when large numbers of staff are working from home and some offices are closed or only partly staffed. In the case of closed offices, it may be sufficient to deploy the same security protocols as are in place in usual times for night-time closures. Where offices are open but only partly staffed, including potentially with fewer security staff in post, then there can be a heightened risk of unauthorised walk-ins. Possible mitigating actions might include:

- Increasing verification checks on entry for example, having more security staff at reception and requiring the presentation of ID, including when access is gained by swiping in.
- Issuing guidance for staff around increased security risks, for example on the importance of locking computers and removing sensitive documents when they are away from their desks; questioning those in the building that they do not know; and reporting any unusual activity.
- Locking unoccupied offices and spaces and locking away unused IT equipment where possible.
- Searching bags and cars exiting from buildings.

Accidental privacy breaches by call centre agents

5. The restrictions on face-to-face interactions as a result of office closures or partial closures has led to a greater demand on call centres. In a service-oriented environment this may increase the pressure on agents to complete more calls, thus creating the potential for mistakes that lead to privacy / confidentiality breaches. This risk could also be compounded where there are staff in place who may be new to, or have limited experience of working in call centres, for example where staff have been redeployed from other areas. It may also be the case that the number of people attempting to obtain information fraudulently in this way will increase as criminals try to exploit vulnerabilities. Possible mitigation actions might include:

- Enhanced guidance to staff about the risks and the importance of following verification and information security requirements.
- Provision of advice on how to deal with callers in distress where there may be more pressure to provide information in violation of security protocols. For example, this may be an area where common scripts might help.
- Clear protocols for inexperienced staff around the number of calls they receive, transferring calls if the conversation becomes more complex or unclear, the caller is in distress or the call centre staff is feeling under pressure. This could be reinforced with training and reminders.
- Pre-screening of calls, with more complex cases or callers in distress being routed to more experienced officers (this may be possible through automated processes through which callers select options).
- Updating of online guidance in light of calls received so that call centre staff or automated response scripts may correctly and consistently answer commonly asked questions and address emerging issues.

Postal mail storage

6. In many tax administrations or tax administration functions, it may not be possible to shift communications from paper to digital without significant changes, including the need for secure digital verification systems.[1] There may, therefore, still be a substantial amount of communications received by post, some of which may be general in nature and some of which may be related to payments and refunds and time-sensitive. (Examples might be where only paper documents are accepted, where original identification documents or other evidentiary documents need to be submitted or where hand written signatures are required.)

7. In some tax administrations, postal mail may be received at office locations that are working with reduced staff numbers. There may, therefore, be significant delays in both opening and processing the documents. In cases of office closure, mail may be put into temporary storage facilities or held at post offices. In addition to the risk of hardship from mail not being opened and processed, storage of unopened or unprocessed mail may increase the risk for loss or theft of postal mail, and, in the latter case, the risk of misuse or public disclosure of taxpayer personal information and possible identity theft.

8. Possible mitigating actions might include:

[1] Data contained in the OECD's 2019 Tax Administration report showed that paper communication continues to be an important way for taxpayers to engage with the tax administration. Table 1.4 of the report shows that twenty-eight administrations reported receiving 66 million paper-based service requests in the fiscal year 2017. While those numbers are slowly declining (-2.9% compared to 2016), paper continues to be more important than email. (see OECD (2019), *Tax Administration 2019: Comparative Information on OECD and other Advanced and Emerging Economies*, OECD Publishing, Paris, https://doi.org/10.1787/74d162b6-en).

- Advising taxpayers to communicate electronically for general or routine communications and not to include sensitive information in such correspondence.
- Distinguishing between general communications and tax sensitive communication through guidance and asking taxpayers to send the latter, where possible, to centres where it can be opened.
- Advising taxpayers and advisers to re-send important documents with appropriate markings on the envelope which can then be sorted or redirected more easily, taking care to not include markings that identify contents for the general public or postal service employees
- Accepting electronic communication such as email (scanned copy) or fax in place of paper documents or original documents. This may require some relaxation of current rules as to the form of communication and documentary requirements (such as acceptance of e-signatures). In this case consideration may also be given to an increase in the number of verifications required or the verification process. (For example, if received electronically more than one form of identification may be required or a control question may be asked from information held by the tax administration.)
- Working with tax crime colleagues to identify markers of identity fraud arising from postal fraud, such as larger than expected numbers of changes of details (addresses, bank accounts) made in a particular area.
- Storing unopened mail in more secure locations rather than storage facilities.

Mailing and shipping procedures

9. The closure of offices and the move to remote working solutions may result in a significant increase in the mailing and shipping of tax information, personally identifiable information, and other sensitive information, to or from remote work locations. This potential increase in the number of deliveries raises the risk and is further increased where there are "no contact" delivery procedures, e.g. packages left outside residences, which are used increasingly during the crisis. Potential mitigating actions might include:

- Issuing guidance to encourage the use of electronic communication to the fullest extent possible (which may require changes in procedural requirements) and providing clarity on situations where it may be necessary to send mail and where it would not be appropriate.
- Using only trusted delivery services that guarantee not to leave mail outside a residence without witnessing the person inside opening the door to collect the mail and have procedures to verify this.

Employee conduct and workspace at home

10. As staff work from home, there may be an increased risk of disclosure of tax relevant and personally identifiable information to family members, cohabitants or visitors. The significant uptake in remote working during this crisis will further increase that risk, particularly in relation to staff who are new to remote working. This could be further compounded by multiple family members or cohabitants now working remotely in the same space or children being at home. The key risk here is that personal information is discussed or worked on, whether physically or online, in the presence of non-government employees.

11. In addition, recent years have seen an increased popularity of smart home technology devices, including virtual assistants that are activated using voice. As staff work from home, such voice-activated assistants increase the risk of inadvertent disclosure of agency matters and taxpayer information as they might be activated accidentally or intentionally and record conversations.

12. Possible mitigating actions might include:

- The issuing of guidance, and possibly remote e-training, around privacy and security risks. This could provide simple examples of how personally identifiable information can easily be revealed in a remote working situation (for example by failure to lock screens when away from the computer, lack of privacy when working, poor password management, etc.).
- This could be reinforced by regular reminders, for example when computers are switched on or as part of regular messaging.
- Ask staff to do a risk assessment of their remote work environment and produce checklists for staff to complete (which could be recorded centrally) on whether they are meeting security requirements. For example, these could ask whether staff: have set a screen lock timer; activate screen lock whenever they are away from the computer; keep passwords secure and regularly change them; have arranged the work station so that conversations cannot be overheard and the screen cannot be viewed by others; keep any sensitive paperwork in locked containers; avoid printing out sensitive information, locking or securing computers and laptops, etc.
- Advising the use of, or providing staff with laptops or computer screens that have anti-spy screen protection that show black screens when looked at from the side.
- Advising the use of, or providing staff with headsets so that bystanders would be unable to listen to calls made or received.
- Providing advice on secure methods of disposing of confidential information, e.g. using scissors to do cross-cut shredding, soaking them in water for a 24-hour period, etc.
- Explaining the risks of virtual assistants and providing guidance to staff on turning off such devices or working in rooms where they are not present.

Storage of IT equipment and records

13. Another risk from remote working is that the personal information of staff, taxpayers, or benefit recipients can be accessible to others because staff members do not have the appropriate facilities to securely store the administration's IT equipment and taxpayer files. While staff with pre-existing remote working arrangements may have administration approved lockable storage cabinets at home, those that are new to remote working may not. The risks are magnified by the number of people moving rapidly to remote working during the pandemic whose homes may not be as secure as the administration's offices. Possible mitigating actions might include:

- Issuing guidance as to how equipment and records might be stored more securely in a home environment, for example in locked rooms, lockable cabinets or inaccessible places.
- Where not already available, asking staff to consider the purchase of computer locks or padlocks where appropriate.
- Where possible, increasing the security of the computer disks through the installation of encryption software.

IT related risks

Use of personal devices

14. While working from home, administration work is typically conducted digitally on the administration's IT equipment and with security controls in place that may prevent staff from using personal devices, for example, printers or scanners, to perform office functions.

15. Staff may be tempted to circumvent those rules by transmitting taxpayer information via unsecured channels to facilitate working in the home environment, e.g. via unencrypted email or other means. This could result in these personal devices introducing malware to the work system and / or personally identifiable information being disclosed to third parties, such as family members or, even hackers if the personal devices are infected with malware or are subsequently stolen. Possible mitigating actions might include:

- Installing software on the administration's computer that detects and prevents non-approved IT equipment from being successfully connected.
- Installing software which prevents sensitive information from being circulated to non-approved email addresses or, where not possible, having prompts that require the sender to declare that the information being sent is non-sensitive.
- Where it is necessary to print out documents, it might be possible for them to be printed by staff who are in the office and sent through secure delivery or allowing staff to reserve time slots during which they could go to the office to print or scan documents (or to destroy them securely).

Phishing attempts

16. The increase in messaging from multiple sources about tax administration operations, situational updates, emergency messages, COVID-19 news, etc. increases the risk of phishing messages being mistaken for official communications and opened by staff or taxpayers. Social hacking is the biggest cybersecurity risk as it places tax administrations at risk for compromised credentials and malware and taxpayers at risk for stolen identities and refund theft. Attempts at phishing may be particularly prevalent in countries where support payments are being delivered through, or with the involvement, of the tax administration. Mitigating actions might include:

- Public messaging as to how recipients of emails purporting to come from the administration can tell if the emails are genuine and listing information that would never be requested by the administration in an email.
- Continuing to communicate clearly and consistently to staff and taxpayers from the same email address.
- Where the administration uses external providers to carry out surveys, (for example, staff or taxpayer surveys) an official message could be circulated in advance to alert those concerned that they will be contacted by an external provider. The message should indicate the name of the external provider and the date when the survey will be circulated.
- Asking staff and taxpayers to report suspicious email by forwarding them to an appropriate administration email account.
- Working with internet service providers on the identification of junk and spam email.

Insecure networks / applications

17. The increase in the use of non-government networks as staff work remotely, poses a risk of information breach. The home networks used by staff to connect their equipment to the administration's IT systems may not have the same level of security (such as firewalls or network intrusion detection systems (NIDS)) compared to the networks used in the administration's offices. This may increase the risk of devices being compromised and information being accessed by unauthorised people. The risk will be even greater where staff considers working from outside the house via public networks, for example to avoid crowded family situations. Similarly, the use of non-government applications, e.g. video conference solutions or file hosting services, may introduce privacy risks as outsiders may listen to conversations or break into virtual meetings. Possible mitigating actions might include:

- Reminding staff to avoid using public networks and only use secure home networks (including regularly updating their home security software).
- Providing guidance for staff of how to protect home networks, including which applications are safe to use.
- Enhancing verification procedures for financial transactions, account access reset, credentials and the sharing of personal information.
- Asking staff to strengthen passwords and, where possible, move to two-factor authentication.
- Considering the options for installing network intrusion detection system (NIDS) remotely, possibly working in cooperation with internet service providers.
- Providing guidance on matters which should not be discussed or transmitted on non-government applications such as video conferences.
- Checking devices on return in case infected with malware.

Human resource related risks

Staff off-boarding

18. Even during the pandemic there will be staff members that leave the administrations either because they are retiring or departing for other purposes. While there is normally a straightforward process in place when it comes to returning badges or equipment, this can prove to be more difficult in times where staff are working remotely and offices are closed. A natural approach to the issue would be the shipping of any material back to the office or the home address of a designated contact person. However, this may create new risks with respect to securing / obtaining the parting staff member's equipment, paper files, identification badges, etc., as material may get lost during delivery. Greater vigilance may be required in the shipping of any materials back to the office / designated staff member to avoid items being lost in the mail. Possible mitigating actions might include:

- Updating procedures for departing staff. For example, the administration could request shipping to be carried out after a designated date via authorised / trusted carriers and require that any devices that may provide access to internal systems, e.g. security tokens, should be shipped separately from laptops.
- Ensuring that the administration's processes allow for complete disabling of the access of departing staff at the end of their contract and prior to the designated date on which equipment/passes etc. will be returned, if earlier.
- Ensuring that any attempt to use ex-staff's credentials are immediately flagged.
- Considering limiting the access of departing staff who are remote working in good time before the end of their contract.

Staff health information

19. Staff have the right to privacy of information pertaining to their health. However, the current crisis is an uncharted territory regarding what information can and should be shared regarding staff who are ill with COVID-19 since it is important information for safety reasons. While some staff may not mind information being shared, others may consider such information private and may be opposed to any sharing.

20. One of the key issues for the administration to consider is the balance between the staff member's personal rights and the safety of other staff members and taxpayers. Careful consideration should be given to when is it important to share a staff member's diagnosis or where they worked / travelled during the past

weeks and, if so, how widely to spread the information. For example, it may not be important information for business continuity reasons (other than for disinfectant purposes) to know that someone has COVID-19 even when they are working in a critical function. It may be sufficient for others involved in the area just to know that the person will not be available for a potentially prolonged period in order to for them to consider how to cover the position. Possible mitigating actions might include:

- Carrying out a data protection impact assessment in order to set out clear rules / protocols to follow as regards the collection and communication of COVID-19 related issues (such as diagnosis or possible diagnosis of staff members or family members). This might involve staff representatives, including unions, as well as data protection officers.
- Communicating the rules / protocols to all staff and providing appropriate reminders.
- Only collecting information to the extent necessary for required purposes and limiting the number of staff who should have access to this information to the minimum necessary, e.g. selected HR personnel.
- Where information has been shared for safety reasons, for example with other staff or taxpayers to enable them to undertake appropriate actions such as testing, quarantine or disinfecting operations, ensure that they understand the importance of keeping the information confidential.
- The staff member concerned should be consulted regarding who the health information will be shared with and for what purpose. The staff member should have control over the sharing of any personal data for optional non-safety related activities such as support, assistance or condolences.

3 Fraud risks

21. The risk of fraud during the pandemic is highly likely to have increased substantially given that, among other things, the situation is fast-moving; there is great potential for misinformation or confusion; there are increased privacy and disclosure risks (as set out in Chapter 2); the routes for fraud may have increased significantly as a result of government payments; there may be reduced controls in place; and compliance and enforcement activity is likely to have been reduced.

22. The risks included in this chapter are grouped into three categories, with the first two risks coming from sources external to the administration and the third category from internal sources:

- ***Identity fraud risks*** – the risks of persons wrongfully obtaining and using data of individuals, businesses or government bodies in fraudulent actions;
- ***Tax fraud risks*** – the risks of individuals or businesses intentionally falsifying information to reduce tax payments, or obtain tax refunds or similar payments; and
- ***Internal fraud risks*** – the risks of fraudulent action by persons that are internal to the administration, such as staff, contractors and other trusted parties.

Identity fraud risks

Individual / business identity theft

23. Many governments have put in place programmes to support businesses and individuals affected by COVID-19 and, in some cases, the tax administration has been tasked with administering the government relief payments. The way such payments are handled may incentivize bad actors to commit individual or business identity theft with the intent to redirect cash payments to their addresses or accounts. This issue may relate to living individuals and active businesses but also to deceased persons or inactive businesses.

24. In addition to the risks related to accessing relief payments, there is also an increased risk that bad actors use the restrictions put on face-to-face interactions and the associated increase in electronic services, to access taxpayer information through identity theft, potentially allowing them to commit tax fraud (such as illicit refund payments) or fraud on third parties (such as banks, mortgage fraud, credit fraud). Possible mitigating actions include:

- Co-operating with other government bodies to verify taxpayer address and account information, such as a national population or business register.
- Using multi-factor authentication for individuals or businesses to access payments.
- Risk assessing whether self-service offerings (such as changes in bank accounts/addresses) should be subject to further verification.

Impersonation scams

25. Another form of identity theft is the impersonation of government bodies, in this case the tax administration, to commit fraud. There are several channels through which those impersonation scams could take place, for example:

- Telephone call scams, where callers claim to be staff of the administration and ask for personal details or direct payment transfers;
- Email scams designed to have taxpayers believe that those are official communications from the administration and containing links to malicious websites; or
- In-person scams, where people pretending to be administration staff knock on doors to collect outstanding payments or request personal information.

26. The COVID-19 government aid programmes increase incentives and opportunities for bad actors to impersonate the administration, for example by pretending to "verify" taxpayer's bank account information. Possible mitigating actions might include:

- Undertaking email or online campaigns warning individuals to be extra vigilant and instructing taxpayers to go directly to the tax administration website in lieu of clicking on links in emails.
- To provide clarity on the form of official communications and interactions, including what the administration will not ask for, as well as common signs of potential fraud.
- Working with government-wide security organisations and internet service providers to shut down fraudulent websites.

Tax fraud risks

Accessing relief or refund payments

27. The government aid programmes, which are often being done at great speed, may incentivise individuals and businesses to commit tax fraud in order to maximise payment amounts or credits. In particular, the high volume of relief or refund requests being made, combined with oversight and control deficiencies which may result from increased remote working, may significantly reduce the robustness of checks. Potential schemes may also involve the creation of new companies to access direct relief payments or obtain tax refunds. Where relief payments are linked to number of employees or employee wages, this may also include recording of fictitious staff.

28. A related issue may be that administrations have provided individuals and businesses with greater ease in complying with tax obligations, such as exempting taxpayers from providing proof based on original documents or allowing the submission of scanned copies. Such simplification may also increase tax fraud risks. In addition, the abilities of banks and other financial institutions to serve as another layer of fraud detection are diminished due to reduced face-to-face services and interactions. The increased use of electronic deposits may decrease the ability to identify suspicious or fraudulent activities.

29. Possible mitigating actions might include:

- Ensuring that all electronic payments are adequately traceable, with particular consideration given to new bank accounts.
- Creating new risk assessment flags for where enhanced checks may be made. These might include: businesses that have been recently formed; taxpayers recently registered with the administration or who have not previously filed; recent changes of bank details or addresses (particularly during the crisis when people are less likely to move).

- Communicating with banks about the importance of verification checks and the application of anti-money laundering rules as well as the reporting of suspicious transactions.
- Communication about the penalties, including criminal penalties, that can be applied for false declarations.

Cash payment related tax fraud

30. The economic crisis caused by COVID-19 and the impact on the finances of businesses may increase the risk of cash payment related tax fraud. Businesses that are still active during the crisis could, for example, sell goods or deliver services against cash payments without handing out receipts thus avoiding tax payments (value added taxes / general sales taxes and income taxes). Another scheme, for those that have employees, could be to pay employees in cash thus avoiding reporting and the related employee withholding taxes and social contributions. Possible mitigating actions might include:

- Alerting businesses of the need to keep records for possible auditing and compliance purposes after the crisis as well as the ability of the tax administration to assess for risk.
- Reminding businesses and employers of the penalties for false declarations.
- Promoting whistle-blowing opportunities.
- Carrying out remote audits or, where possible, physical audits when there is a strong reason to suspect fraud.

Internal fraud risks

31. The COVID-19 situation is difficult for many people including those that work in tax administrations or provide contracted services. Social distancing rules and remote working may have negative effects on morale and may increase psychological stress faced by staff, contractors or other trusted partners. In addition, some of those stakeholders (including staff relatives) may also face financial pressure as a result of the crisis.

32. Increased financial pressure mixed with rapid changes and programme rollouts as well as sometimes limited supervision as a result of remote working, may provide the opportunity and motive for some staff to commit fraud through sharing of taxpayer or staff information, or by engaging in intentional misconduct to misappropriate government resources or assets. While highly unlikely, the impact of any such fraud on the tax administration's reputation could be very damaging.

33. Possible mitigating actions might include:

- Setting-up and regularly advertising special support programmes for staff, and encouraging managers to check-in frequently with their teams. Such programmes could also help staff under financial pressure.
- Conducting internal fraud risk assessments or deploying internal fraud risk self-assessment tools, for example requiring staff to disclose certain investments.
- Increasing the checks required over certain thresholds for paying out money to taxpayers, for example a "four eyes principle" (where certain activity must be approved by at least two people) could be applied for significant amounts.
- Advising managers to be vigilant and to ensure that internal control / audit trail checks are conducted and ensuring a systematic sharing of results of remote activities.

Contact

OECD Forum on Tax Administration Secretariat (✉ FTA@oecd.org)

www.oecd.org/tax/forum-on-tax-administration/