HMRC Data Protection Impact Assessment (DPIA) template	
Title of data processing activity / system	Transaction Monitoring (TxM)
DPIA co-ordinator (the person completing this template)	Service Owner Transaction Monitoring
DPIA Owner (e.g. project leader, asset or process owner)	Transaction Monitoring Team
Business Area	CDIO Customer Compliance Group Vertical
DPIA reference number (allocated by your SIBP team – save this in the doc file name)	024
DPIA Version control: For instance v. 1.0, 1.1, 2.0 etc.	3.1 This published version has been edited where appropriate when inclusion of those details would be likely to prejudice the purposes of transaction monitoring and/or undermine HMRC's security
Date DPIA was last reviewed	18/03/2019
Please indicate all that apply with inserting a 'X' in the box	This is (double click to check or uncheck boxes): ☐ A new Programme, Project, system or data processing activity ☒ An existing system or data processing activity ☐ Sharing personal information with a third party ☐ Other. [Please insert here].
Please provide some context to the service/system/process the DPIA relates to	Transaction Monitoring (TxM) records customer activity across HMRC customer facing services. It then processes activity in order to detect suspicious behaviours which might indicate fraud or crime.

Screening questions (Q1-12)	**Notes for completion** – The screening process only needs to be completed once. If you answer yes to one or more of these questions, you must consider carrying out a full DPIA (Q13-26 of this template) for the Programme / project or data processing activity.	**Y/N**
1. Does the processing activity or system involve any personal data?	Personal data means any information relating to an identified or identifiable individual, e.g. National insurance number or name/address, email address etc. Full DPIAs may be required for systems or activities which will be or have been specifically designed to process personal data and for data sharing agreements with third parties. DPIAs should be commenced as early as possible in the design process, preferably at a pre Change Framework stage. They are not necessary for systems which contain no personal data other than for administrative purposes, or for routine processing activities e.g. the collection of staff information to organise a conference, or for disclosure of personal data to an agent following the receipt of a form 64-8.	
TxM captures comprehensive data for every customer and every submission to HMRC. This may include names, addresses, bank account details, tax identifiers, geolocations, IP addresses, device identification features, contact details, tax submissions, variations, changes of circumstances etc. It is specifically designed to capture and analyse a wide range of personal data in order to detect and prevent unauthorised access and crime.		Y

2. Does the processing activity involve new technology, IT systems or change requests to existing systems?	A full DPIA (Q13-26 of this form) is required if the processing involves new technologies (e.g. Smart technologies) or the novel application of existing technologies (including AI). In HMRC new departmental IT systems including large scale personal data systems and national databases, must have a full DPIA. The risk may be higher if the data processing activity involves using data in innovative ways, e.g. pre-population. Consider whether a DPIA is required for new data storage solutions, e.g. digitisation of personal data held on paper, or migration of large volumes of data between systems or to the cloud. In all cases consider whether the volume, sensitivity and range of personal data increases the data protection risk and justifies a DPIA.	
TxM replaced a Legacy system 4 years ago. Sections 2-6 are completed accordingly.		Y
3. Is the processing activity related to a strategic or policy led initiative?	For instance new requirements from the UK Government or Cabinet Office may have data protection implications, especially if they require a new system or process involving personal data. The risks are likely to be higher if the initiative requires the innovative use of personal data or new technological or organisational solutions.	
The activity is related to the National Cyber Security Strategy and is in line with National Cyber Security Centre good practice guides GPG53, (the good practice guide for Transaction Monitoring) and GPG43 (requirements for secure delivery of online public services). Collection of TxM data is mandated in API channels via Statutory Instrument (The Delivery of Tax Information through Software (Ancillary Metadata) Regulations 2019).		Y
4. Does the processing activity involve the collection of new categories of personal data for an existing or new process?	This may apply to a new processing activity involving the collection of new categories of data, or to an existing process which is being adapted. If you answer yes, the volume of personal data, sensitivity and range of data items being processed and the duration of the data processing activity will partly determine the level of risk and whether a DPIA is necessary. The data protection risk may also be increased if it involves new data *and* new technology.	
These classes of data have been collected for over 10 years. HMRC's Privacy Notice informs customers about how their personal information is used.		Y
5. Could the processing activity be considered intrusive or require contact with individuals	If any consultation has been carried out it will provide supporting evidence. Consider whether the medium (post, email, SMS, telephone etc.) might be considered intrusive. DPIAs are recommended for 'invisible processing' of personal data – that is data which has not been obtained direct from the data subject and where providing the privacy notice information (required by GDPR Article 14) would prove impossible or involve disproportionate effort.	

in ways that they might find intrusive?	Consider potential reputational risks to HMRC, e.g. if public concern is raised over the processing activity, or the impact on a particular group of vulnerable data subjects. Consider whether the volume, sensitivity, range of personal data and the duration of the activity increases the data protection risk and justifies a DPIA.	
Customers are made aware of their transactions being monitored by means of a published fair processing notice. Notifying customers of the specifics of Transaction Monitoring and how we use it would undermine the primary purpose of the system, which is to detect and prevent crime. TxM are not required to seek consent from customers. The TxM team have no contact with customers.		Y
6. Is the personal data being disclosed to external organisations or people (not suppliers)?	Formal Data Sharing Agreements and Memoranda of Understanding (MoU) involving external exchange of personal data with other Public Sector Bodies or other government departments must have a DPIA. And DPIAs should be considered for any data sharing activities with third parties, especially if the potential impact to individuals would be high if there was a data breach. The focus of this question is on data shares other than suppliers running HMRCs systems. Specify if there is a contract or data sharing agreement. Consider whether the volume, sensitivity, range of personal data and the duration of the activity increases the data protection risk and justifies a DPIA.	
Some very limited personal data may be disclosed to 3rd parties as part of the processing such as sharing IP addresses with National Cyber Security Centre to detect fraud. TxM may share confirmed fraud flags with other government departments, the Police and the National Cyber Security Centre.		Y
7. Does the processing activity use systematic and extensive profiling or automated decision-making to make significant decisions about people?	Automated processing, including 'profiling' is when decisions are made about individuals' **solely** by automated means. For a processing activity to be classified as automated profiling, including 'profiling', there must be no human intervention in the decision making process (e.g. no appeals process) and the decision will have a serious negative impact on the individual. Profiling means evaluating a data subject by any form of **automated** process to analyse or predict aspects such as performance at work, economic situation, health, behaviour, location or movements. Profiling can be of a particular group or demographic. Where appropriate a customer privacy notice should explain the activity and a DPIA should be carried out if this is not possible. DPIAs must be carried out if profiling or special category data is used to decide on access to services, or if profiling is carried out on a large scale, or on vulnerable data subjects (including children).	
TxM builds profiles of customer activity. These profiles generate alerts which inform a human being, who will make a decision. TxM may influence how transactions are processed by routing them for review by risk specialists. HMRC has a published privacy notice and this DPIA, although no special categories of data are included		N
8. Does the activity involve	The purpose limitation principle specifies that data must be collected for a specified, explicit and legitimate	

re-purposing personal data or combining it with another dataset for another use?	purpose. Consider whether any re-purposing or matching of data has a lawful basis for processing in accordance with HMRCs functions. When HMRC obtains information for one of our functions under the Commissioners for Revenue and Customs Act 2005, that information may be used for any of our other functions. You can find details about HMRC's legal basis for processing information on the GDPR Knowledge Hub. Also consider whether personal data shared with and used by third parties is compatible with the original purpose or purposes for processing. A DPIA is required for the re-use of publicly available personal data. A DPIA is not necessary for anonymised data.	
TxM is designed to capture and analyse a wide range of personal data in order to detect and prevent unauthorised access and crime. This may involve the repurposing of data, and combining it with other data. HMRC's lawful basis for processing the data is Article 6(1)(e) - public interest, i.e. protecting the public purse and confidential customer data.		Y
9. Does the activity involve the systematic monitoring of public areas on a large scale?	This would include all forms of tracking and profiling on the internet, e.g. data aggregation, cookies and mobile apps, also CCTV in public places. Consult your SIBP team for further advice if the activity involves systematic monitoring.	
TxM monitors, tracks and records traffic for every HMRC customer across all HMRC channels and services.		Y
10. Does the activity involve processing on a large scale of special categories of data, or of personal data relating to vulnerable subjects or criminal convictions?	A full DPIA must be carried out if special category data (data about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation) is used for profiling activities (see Q7) or if we plan to process special category data or criminal data on a large scale. A full DPIA must be carried out if any biometric or genetic data is processed on a large scale. A full DPIA is recommended if the processing involves vulnerable individuals including children. Consider whether the volume, sensitivity, range of personal data and the duration of the activity increases the data protection risk and justifies a DPIA.	
In the case of a change to sexual orientation, HMRC services update their records outside of the TxM process. There is a residual risk that where someone undergoes gender reassignment, records may be kept showing their previous gender in the customer's history in internal TxM. No special category data is used for profiling purposes in internal or external TxM. The amount of data held in TxM makes it possible for personal data relating to vulnerable subjects to be used in processing. TxM holds no data on criminal convictions. TxM holds data about confirmed fraud attempts and fraud risk.		Y
11. Does the activity involve	Refer to the list of countries outside the EEA evaluated by the European Commission as having an adequate level of	

transferring personal data to a non EEA country?	data protection (see definition of Adequacy). Offshoring may apply to web apps and online cloud based services depending on where the data is processed and stored. All Offshoring must comply with the HMRC Offshoring policy regardless of where it is being transferred to. See also ICO guidance: International transfers.	
TxM Device Profiling features use a 3rd party in order to develop a reliable device identification. 3rd Party data centres are located in the USA – Portland, and Seattle. Data may also be stored in Satellite data centres in Miami, and Amsterdam in the Netherlands. The 3rd Party is US-EU Privacy Shield certified. **Range of Data offshored**: Device Fingerprint (Browser Specification, OS version, Installed Apps, User Agent String etc), Client IP Address (as presented to HMRC), Customer ID (TxM Specific Customer ID used for internal correlation in TxM). **Volume:** Every time a user logs into HMRC web-based systems, some or all of the above range of data may be transmitted to the supplier. **Duration**: Where fraud is confirmed against a device profile, the supplier retains records for 5 years from the date last seen. In all other cases the 3rd party retain device profile information for 2 years. **Sensitivity**: Data shared with 3rd party is of limited sensitivity as the only personal data contained is IP address. A unique HMRC customer ID is shared but this is only used for internal correlation within TxM and not used for any other service. All other data relates to the characteristics of the computer in use by the customer. The 3rd party may not share HMRC data with any other 3rd party except in cases where fraud against HMRC is confirmed. Where fraud is confirmed the 3rd party may share a fraud flag with other 3rd parties for the prevention and detection of crime.		Y
12. Based on your answers to questions 1 to 11, on balance is the processing activity likely to result in a high risk to the rights and freedoms of individuals?	Processing activities likely to result in a high risk to the rights and freedoms of individuals must have a full DPIA (Q13-26 of this template), particularly if misuse of the personal data may endanger an individual's physical health or safety. The data protection risks to the rights and freedoms of individuals are determined by your answers to Q1-11 (above). If more than one of the above criteria applies to an activity, the risk may be cumulatively higher and this will be a prioritising factor to carry out a DPIA. Always consider whether the volume, sensitivity, range of personal data and the duration of the activity increases the data protection risk and justifies a DPIA. Do a full DPIA if there are any known high data protection risks (e.g. non-compliance with data retention policies). If it is not clear whether there is a high risk or not, consult your SIBP team and if it is still unclear carry out a full DPIA. If you think a DPIA already exists for a similar processing activity with a similar high risk, consult your SIBP team for advice. **If you consider that a full DPIA is not required, provide your justification below in enough detail to enable external bodies, such as the Information Commissioner's Office, to fully understand why the Data Protection and privacy risks are not sufficiently high to warrant one.**	
TxM may collect, record and retain information regarding every customer interaction and transaction with HMRC Services. The data collected includes large volumes of personal data from all HMRC digital channels.		Y
DPIA screening approved by [name]. This should be the DPIA owner (e.g. project leader, asset or process owner in the business). Seek the advice of your SIBP team if the screening decision for a full DPIA is unclear.		Date

Service Owner Transaction Monitoring	18/03/2019

**** ONLY COMPLETE QUESTIONS 13 TO 26 OF THIS TEMPLATE IF THE SCREENING QUESTIONS 1-12 INDICATE THAT A FULL DPIA IS REQUIRED ****
IF THE FULL FORM IS COMPLETED IT MUST BE REVIEWED AND MAINTAINED FOR THE DURATION OF THE PROCESSING ACTIVITY

Q13-17. Overview of the Data Processing system or activity including the data flows	**Notes for completion**
13. Provide a brief overview of the data processing system or activity and why it is needed.	a). Include an overview of the purpose of the processing activity, including what HMRC function it supports. The purpose relates to the expected benefits for HMRC, including any intended outcomes for individuals. b). Include an overview of the context the processing activity to demonstrate the relevant internal and external factors which may affect expectations or impact, e.g. any issues of current public concern. c). Include an overview of the nature of the processing activity, particularly how the data is sourced, collected, stored, used, who has access to it, and who it is shared with. d). Include an overview of the scope of the processing activity, particularly the sensitivity of the personal data, the extent and frequency of processing, the duration of the processing and geographical area covered. Include a summary of the volume and variety of the personal data. Data categories could include: • Name, address, date of birth, email, telephone recordings, IP address or other online identifiers • NINO or other type of reference number • Banking transactions, tax, tax benefit information • Sick Absence Records, health data, religion, ethnicity • Workplace related such as performance data

TxM may collect, record and retain information regarding every customer interaction and transaction with HMRC Services

Sources
Internet and software based direct interaction to HMRC services
Telephone based direct contact to HMRC services
Paper based direct contact to HMRC services

Data may include

- Name, address, date of birth, email, telephone number, IP address or other online identifiers, telephone number
- All classes of tax identifier
- Banking transactions, tax and benefit information
- Risk information and fraud indicators from HMRC business areas and 3rd parties

Data may include any information submitted via any channel for all classes of customer.

Information is captured and recorded 24/7/365.
Information is recorded and retained for 6 years +1 (6 years plus current year)

The purpose of Transaction Monitoring is to identify suspicious or anomalous activity which could indicate unauthorised access, compromise of customer accounts, or fraudulent submissions to HMRC.

14. Who is the controller for the information to be processed? Please indicate all that apply with inserting a 'X' in the box	A data controller is any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. All government departments are controllers in their own right. A data processor is responsible for processing personal data on behalf of a controller.

The Data Controller is (double click to check or uncheck boxes):

☒ HMRC only
☐ Another organisation only – [insert name of organisation]
☐ Other organisations only – [insert names of all of the other organisations]
☐ HMRC and a joint controller [insert name of other organisation(s)]
☐ Not yet known – [insert here why not known]

15. List all the main recipients of the data, their role in the processing activity and their relationship to each other.	Consider where the data flows from and to. Data recipients may include: data subjects', HMRC business areas, other government departments and third parties such as software developers, banks, suppliers, delivery partners or agents. Include details of data processors and specify whether there is a contract or data sharing agreement. Information about who we share the data with should be in the customer privacy notice if there is one. If HMRC is a joint data controller you should note here who does what, including which party will be responsible for the measures designed to treat risks. Attach a flow diagram to illustrate the relationships if this is more helpful (recommended where there are complex flows involving many parties).

Inside HMRC we share TxM data with:
Risk Intelligence teams – To detect and prevent fraud against HMRC systems

Fraud Investigation Teams – To investigate and prosecute fraud against HMRC. Summary data may be shared with wider HMRC on a limited basis, to provide service specific information about customer usage of digital services. We may share TxM data with other government departments, the Police and the National Cyber Security Centre for the purposes of prevention and detection of crime.

16. Describe the infrastructure and assets on which the data processing activity relies.	Consider IT systems, hardware, software, operating systems, business applications, people, paper, where the data is stored and transmission channels used.

TxM is hosted in dedicated HMRC secure data environments. These services are built managed and maintained by HMRC. TxM service security is regularly tested and assured by independent 3rd parties. We security vet all personnel who manage TxM including HMRC staff and any 3rd party contractors. All communication channels to and from TxM are encrypted with SSL/TLS or VPNs. Connections are limited to known sources and devices. TxM Data is encrypted at rest.

17. Approximately how many individuals are affected by the activity?	Consider HMRC staff and external customers. If not known, use best approximation or a description, e.g. 'all taxpayers', 'all HMRC staff', 'under 1000' etc.

Approximately 10000 HMRC staff have access to TxM. All HMRC customers will be impacted by information stored in TxM.

Q18-23. Applying the Data Protection Principles	**Notes for completion**
18. What is the lawful purpose for the data system or processing activity?	Refer to the Lawful basis for processing, explained by GDPR Article 6. HMRC carries out most functions in the public interest or to comply with a legal or contractual obligation. HMRC will rarely rely on consent. Details of HMRCs lawful basis can be found on the GDPR Knowledge Hub. Provide any further details of HMRCs legislative or legal basis for the data processing activity (i.e. the basis for processing under Commissioners for Revenue and Customs Act 2005 or any other enabling legislation). Consider any data sharing agreement in place which specifies the basis for sharing. Describe any other reason why the processing activity is being carried out. If necessary seek advice from your SIBP team about processing activities relating to special category data and/or criminal offence data or processing for law enforcement purposes (DPA 2018 Pt3). This

	information would be included in any Privacy Notice. Refer to the HMRC Privacy Notice for more information.

Please indicate the lawful basis for processing by inserting an 'X' in any boxes that apply (double click)

☒ Personal data is processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in HMRC
☐ Personal data is processed to comply with a legal obligation to which HMRC is subject
☐ We are processing personal data for the performance of a contract
☐ We are processing personal data with customer consent
☐ We are processing personal data for law enforcement purposes
☐ Other.

HMRC processes TxM data in performance of its Public task (Article 6(1)(e) of the GDPR)

HMRC require third party software developers to provide additional metadata for the furtherance of our Public task. The collection and supply of this data is mandated by Statutory Instrument. (The Delivery of Tax Information through Software (Ancillary Metadata) Regulations 2019).

19. Describe any measures to ensure data processing is limited to what is necessary and proportionate for the lawful purpose	Consider whether the processing actually achieves your purpose, or whether there is another less intrusive way to achieve the same outcome. The processing activity should be compatible with the purpose for which the data was first collected (purpose limitation). Are there measures to prevent function creep? The processing activity should be designed to use only those categories of data which are necessary to achieve the policy/delivery/operational aim. How will you ensure data minimisation? Can the data be anonymised, either partly or wholly and still achieve the policy/delivery/operational aim? Consider whether there is a contract or data sharing agreement which specifies how data can be used. What measures do you take to ensure processors (third parties) comply?

TxM data is collected in performance of HMRCs public task, and for the detection and prevention of crime.
All users with access to TxM data are vetted and access is limited by task.
All users are required to have a business reason for access, which has to be confirmed by line management before access is granted.
Where data from TxM is shared with external services, it is limited to the minimum dataset required to complete the function.
The creation of accounts and the privilege and access on accounts is managed by a separate operation teams. There is a separation of duties between the people who create accounts and the people who use the accounts.
All access to TxM data is audited and monitored by HMRC.

Existing security measures provide for authentication of customers before they establish access to their records. Authentication alone does not provide sufficient protection to prevent unauthorised access to customer accounts.

Despite authentication customer credentials can be stolen and abused by online criminals. A customer's own computer and system can also be targeted by online

criminals, who use viruses and malware to take control of computers, impersonate legitimate customers and unlawfully obtain funds from HMRC. As a result authentication alone does not provide sufficient protection to prevent unauthorised access to customer accounts. HMRC therefore needs to monitor digital channels using TxM. This enables HMRC to establish normal behaviours for customers and detect abnormal or suspicious activities. Early warning signs are then used by HMRC to detect and prevent fraud and protect customer accounts and personal information. TxM data is used to identify suspicious behaviours and activities which could indicate fraud. Where such activities are detected, TxM influences the processing of transactions to ensure they are reviewed by HMRC Preventative Risking staff. Where risking staff confirm an alerted activity is fraud, they take action to protect the customer account, notify the customer as appropriate, and suspend any repayments fraudulently claimed. TxM relies on metadata surrounding transactions in order to detect anomalous behaviours. Without this data TxM would not be able to perform its primary function The metadata set required to be collected by software developers has been selected after careful consideration by HMRC of the data set required in order to establish a reasonably accurate behaviour pattern for a Making Tax Digital (MTD) customer or group of MTD customers and allow HMRC to effectively monitor and protect access to MTD customers' data. The TxM metadata set represents the minimum amount of data HMRC needs to carry out TxM. There is no other less invasive way of achieving the same objective and outcome of protecting the confidentiality of its customers' data within the structure of the Making Tax Digital programme. HMRC has considered the use of digital certificates instead of transaction monitoring, but concluded they are insufficient for securing the safety of customers' data. Digital certificates are primarily used for non-repudiation or authentication purposes, which are able to identify a client account or machine, but do not indicate whether a client account or machine has potentially been compromised. The processing is proportionate because there is no alternative approach to TxM which could reasonably and reliably achieve the same primary purposes	
20. Describe any measures to ensure the data is kept accurate, up to date and secure	Consider the confidentiality, integrity and availability of the data. Measures may include: • Security and confidentiality: authentication, password control, encryption, data separation, network security, maintenance / patching, pseudonymisation, staff vetting, administrative and user controls, security risk assessment, physical access controls, paper document security, SIBP team consultation and whether accreditation has been given (and by whom) for the sensitivity of data being processed • Integrity and data quality: how the data will be kept up to date and accurate including how it can be checked or verified, e.g. via auditable logging. Specific considerations include data validation rules and processes for data rectification. An example might include: providing a self-service facility which allows the customer to update (certain) information themselves, particularly for online services • Availability: Business Continuity arrangements, data backup, third party assurance Consider relationships with & assurance of third parties. Consider any additional measures in place for more

	sensitive data such as special categories of data or criminal conviction data.
Data is received and processed in real time. As soon as data is received, it is replicated 7 times and the system regularly compares the 7 copies to ensure accuracy and integrity is maintained. TxM backs up data on an hourly basis to an offline back up storage in the UK. If the TxM service/ any of its communication channels are unavailable, all data feeds cache data until TxM is available again. This data is then consumed into the system. TxM is subject to penetration testing of all of their systems and connections to other systems on a 6 monthly cycle. Penetration testing uses trusted experts in information security risk, to try to access TxM through unauthorised routes. This tests our security measures and ensures we stay up to date. All development work is reviewed by internal peer review. This helps reduce the risk that a single programmer could develop malicious code and add it to our systems. There is secure deployment pipeline. This helps prevent developers from directly adding software to our production systems without authority. TxM audits all HMRC user activity across the system.	
21. Are effective data retention schedules planned/implemented for the system or activity, including for third parties?	Personal data must only be retained for as long as it is needed. Manual or automatic data disposition processes can be applied. Assurance activities must ensure that retention policies and schedules are up to date and adhered to by all parties. Details of data retention policies must be included in the Privacy Notice if there is one. HMRC has published its Records Management and Retention and disposal policy on GOV.UK and business areas maintain retention schedules. Consider how data disposition activities work for the processing activity and how data is securely destroyed. Your SIBP team can provide further advice.
Data Retention is 6 years + current year in accordance with the HMRC records management and retention and disposal policy. , in line with the legal requirement for retention of tax records	
22. Describe how the rights of the data subject have or will be designed into the system or activity, including how requests from data subjects will be handled.	Consider how you will support the data subjects' rights. The individual rights of data subjects' include: right of access, right of rectification, right of erasure, right of portability and the right to object to processing. HMRC must be transparent about the use of powers. Consider how customers and staff will be made aware of what is happening to their data at the point of collection, including any relationships with processors (e.g. via a privacy notice or guidance). HMRC has existing procedures to respond to Subject Access Requests within one month of receipt. Consideration should be given to how data can be extracted for SARs requests. Be aware of cross government exchanges of information and identify responsibilities for who takes the lead in answering SARs.
TxM data is collected as part of HMRC's public task.(Article 6(1)(e) of the GDPR) Data subjects are able to make requests via the normal HMRC channels. However, exemptions from data subject rights will apply where their application would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty or an imposition of a similar nature as per Schedule 2 of the data Protection Act 2018. Disclosure of TxM data would undermine the primary purpose	

of the system.	
23. If personal data is being transferred to a non EEA country, what safeguards have been considered or implemented?	Provide the names of third countries or international organisations that personal data are transferred to. How do you safeguard international transfers? Consider the confidentiality, integrity and availability of the data. Consider any specific safeguards for third parties. Refer to the HMRC Offshoring policy and ICO guidance. If there is a Privacy Notice it should say whether data will be transferred to a third country, including what safeguards are in place for international transfers.
TxM Device Profiling features use a 3rd party in order to develop a reliable device identification. 3rd Party data centres are located in the USA – Portland, and Seattle. Data may also be stored in Satellite data centres in Miami, and Amsterdam in the Netherlands. The 3rd Party is US-EU Privacy Shield certified. **Range of Data offshored**: Device Fingerprint (Browser Specification, OS version, Installed Apps, User Agent String etc), Client IP Address (as presented to HMRC), Customer ID (TxM Specific Customer ID used for internal correlation in TxM). **Volume:** Every time a user logs into HMRC web based systems some or all of the above range of data may be transmitted to the supplier. **Duration**: Where fraud is confirmed against a device profile, the supplier retains records for 5 years from the date last seen. In all other cases the 3rd party retain device profile information for 2 years. **Sensitivity**: Data shared with 3rd party is of limited sensitivity as the only personal data contained is IP address. A unique HMRC customer ID is shared but this is only used for internal correlation within TxM and not used for any other service. All other data relates to the characteristics of the computer in use by the customer. The 3rd party may not share HMRC data with any other 3rd party except in cases where fraud against HMRC is confirmed. Where fraud is confirmed the 3rd party may share a fraud flag with other 3rd parties for the prevention and detection of crime.	
Consultation	**Notes for completion**
24. Describe the approach to consultation and the main outcomes if already carried out.	Decide who should be consulted internally and externally, how the consultation will be carried out, and for what purpose. If this is part of a Programme or project it should be part of the overall plan. Internal consultation may be appropriate to identify and mitigate the risks. Stakeholders might include: data subjects', business areas, governance groups, Solicitors Office, other government departments, subject matter experts, digital security managers, risk managers, data processors and your SIBP team. External consultation will not always be necessary.
TxM is an established HMRC system.	