HM Revenue
& Customs

Transparency data

Memorandum of Understanding: accessing HMRC information for appointments to the House of Lords

Updated 2 September 2024

Contents

This publication is available at https://www.gov.uk/government/publications/sharing-hmrc-information-to-assist-in-appointments-to-the-house-of-lords/c673bd6e-f299-4528-8372-080fed9c2bc8

1. Introduction

This Memorandum of Understanding (MoU) sets out the information sharing arrangement between HMRC and the House of Lords Appointments Commission. For the context of this MoU ‘information’ is defined as a collective set of data and/or facts that when shared between the participants through this MoU will support the participants in delivering the purpose of the data sharing activity described below.

Information will only be exchanged where it is lawful to do so. The relevant legal bases are detailed within this agreement. It should be noted that ‘exchange covers all transfers of information between the participants, including where one participant has direct access to information or systems in the other.

This MoU is not intended to be legally binding. It documents the respective roles, processes, procedures, and agreements reached between HM Revenue and Customs (HMRC) and the participants. This MoU should not be interpreted as removing, or reducing, existing legal obligations or responsibilities of each Participant, for example as Controllers under the UK General Data Protection Regulations (UK GDPR).

2. Purpose and benefits of the data sharing agreement

The commissioners believe that the disclosure of information to House of Lords Appointments Commission is necessary and proportionate because it is to inform the Commission on whether a nominee’s tax affairs are in order, which is necessary to fulfil HMRC functions of collecting and managing revenue by:

- increasing the likelihood that the individual subject to the HMRC check will ensure that their tax affairs are in order and up to date
- increasing the likelihood that other individuals in a similar position will be influenced to rectify their tax affairs if they become aware that poor tax behaviour is not consistent with the award of an honour
- increasing the likelihood that taxpayers at large will maintain their trust in the integrity of tax administration by HMRC and comply with their tax obligations voluntarily if tax behaviour is seen as a factor when considering public reward and recognition via the honours system
- reducing the likelihood that taxpayers at large will lose their trust in the integrity of tax administration by HMRC and so fail to comply with their tax obligations voluntarily. Trust would likely be lost if an honour was awarded to someone with negative tax behaviours and those behaviours became

linked to the positive recognition that accompanies the award of an honour

House of Lords Appointments Commission considers that the disclosure of information to HMRC is necessary and proportionate because, as part of its vetting process, probity checks are carried out to minimise the risk that prospective nominees have behaved in ways likely to bring the House of Lords into disrepute. This is intended to ensure life peers are in good standing and to protect the integrity of the House of Lords. In turn, this serves to provide public assurance about standards in public life and the good governance of the UK.

The purpose of this MoU is to set out the arrangements for the exchange of information between HMRC and House of Lords Appointments Commission in relation to checks undertaken prior to making decisions about peerages.

Where a check has been carried out, House of Lords Appointments Commission will take the risk rating from HMRC into account together with other information in order to reach a decision on whether to offer support to the nominee in the Commission's advice to the Prime Minister.

House of Lords Appointments Commission requests Government departments including HMRC undertake checks on individuals in order to provide accurate vetting information on the suitability of individuals for a peerage. Life peerages are granted to individuals nominated primarily by political parties or by House of Lords Appointments Commission (as crossbench peers), and in order to provide an ongoing role in public life for individuals such as former MPs, senior judges, and other senior public officials. The vetting carried out by House of Lords Appointments Commission is in place to minimise the risk that prospective nominees have behaved in ways likely to bring the House of Lords into disrepute. House of Lords Appointments Commission protects the integrity of the House of Lords by carrying out probity checks on nominees submitted by the Prime Minister, before providing them with a vetting report that states whether nominations can be supported by the Commission. The Prime Minister then decides whether to recommend their nominations to HM The Sovereign for approval.

Nominees are made aware that they have been nominated and provide their signed consent for the probity checks to be carried out. Under paragraph 15 of Part 2 of Schedule 2 to the Data Protection Act 2018, the same requirements of UK GDPR are disapplied where personal data is processed for the purposes of the conferring by the Crown of any honour or dignity; this includes the requirement for advance consent of the data subject. A peerage is a dignity. However, applicants' consent is sought because a life peerage together with introduction to the House of Lords confers a lifelong role in the UK's legislature. Applicants must provide their consent to abide by conditions of membership of the Lords such as ongoing residency for tax purposes.

Special Data Protection Act 2018 provisions for honours and dignities do not remove the duty to comply with the data protection principles, including the obligations that data is processed lawfully (under an identified legal base), that it is only collected for specified purpose(s), that it is adequate and relevant to that purpose, that it is accurate and kept up to date where necessary, that it is only kept for as long as it is needed for that purpose (unless forming part of the historic record), and that it is kept secure; among other data protection requirements.

Nominees are aware that a check with HMRC forms part of the vetting process. It should be clear to the potential nominees that poor tax behaviour is not consistent with the award of a peerage. All information about a peerage nominee, received from any source, is treated in the strictest confidence by House of Lords Appointments Commission and others involved in the vetting process.

The benefits of disclosure by HMRC are enhanced by the existence of these checks being in the public domain on GOV.UK, so that those nominated for a peerage (and hence potentially subject to an HMRC check); individuals in a similar position; and taxpayers at large may become aware that HMRC carries out checks to inform the recommendation to award a life peerage.

The benefits to HMRC functions outlined in the above sections can be achieved through minimal disclosure of information in the form of a risk rating of low, medium and high reflecting the categories in the Annex to this MoU and without disclosing any underlying detail about the tax affairs of an individual being considered for a peerage.

3. Relationships under UK GDPR in respect of any personal data being exchanged under this agreement

HMRC and the House of Lords Appointments Commission

Status of HMRC under UK GDPR in respect of any personal data being processed under this agreement

HMRC will be disclosing and receiving personal data under this agreement.

Where personal data is being disclosed under this agreement, HMRC status will be a controller because HMRC alone determines the purpose and means of the processing of personal data.

Where personal data is being received under this agreement, HMRC status will be a controller because HMRC alone determines the purpose and means of the processing of personal data.

House of Lords Appointments Commission under UK GDPR in respect of any personal data being processed under this agreement

House of Lords Appointments Commission will be disclosing and receiving personal data under this agreement.

Where personal data is being received under this agreement, House of Lords Appointments Commission status will be a controller because they alone determine the purpose and means of the processing of personal data.

Where personal data is being disclosed under this agreement, House of Lords Appointments Commission status will be a controller because they alone determine the purpose and means of the processing of personal data.

4. Handling of personal data and security

Where Participants bear the responsibility of a Data Controller they must ensure that any personal data received pursuant to this MoU is handled and processed in accordance with the current seven UK GDPR principles (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/).

Additionally as part of the Government, HMRC and House of Lords Appointments Commission must process personal data in compliance with the mandatory requirements set out in HM Government Security Policy Framework (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework) guidance issued by the Cabinet Office when handling, transferring, storing, accessing or destroying Information assets.

Participants must ensure effective measures are in place to protect personal data in their care and manage potential or actual incidents of loss of the personal data. Such measures will include, but are not limited to:

- personal data should not be transferred or stored on any type of portable device unless absolutely necessary, and if so, it must be encrypted, and password protected to an agreed standard

- participants will take steps to ensure that all staff involved in the data sharing activities are adequately trained and are aware of their responsibilities under the Data Protection Act, UK GDPR and this MoU
- access to personal data received by Participants pursuant to this MoU must be restricted to personnel on a legitimate need-to-know basis, and with security clearance at the appropriate level
- Participants will comply with the Government Security Classifications Policy (https://www.gov.uk/government/publications/government-security-classifications) (GSCP) where applicable

Duration of the data sharing

Start date of agreement: 5 May 2023
End of date agreement: 5 May 2028

A review will take place on 5 May 2025.

5. Legal basis and lawful basis

HMRC has specific legislation within the Commissioners for Revenue and Customs Act (2005) (https://www.legislation.gov.uk/ukpga/2005/11/contents) which covers the confidentiality of information held by the department, when it is lawful to disclose that information and legal sanctions for wrongful disclosure. For HMRC, disclosure of information is precluded except in certain limited circumstances (broadly, for the purposes of its functions, where there is a legislative gateway or with customer consent. Unlawful disclosure relating to an identifiable person constitutes a criminal offence. The criminal sanction for unlawful disclosure is detailed at section 19 of the Commissioners for Revenue and Customs Act 2005.

Data can only be shared where there is a legal basis for the exchange and for the purposes described in this MoU. No data should be exchanged without a legal basis and all exchanges must comply with our legal obligations under both the Data Protection Act 2018 and Human Rights Act (HRA) 1998.

Section 18 of the Commissioners for Revenue and Customs Act 2005 (‘CRCA’) places HMRC under a statutory duty of confidentiality not to disclose information it holds in connection with its functions except in the circumstances permitted by section 18. Unlawful disclosure relating to an identifiable person constitutes a criminal offence. The criminal sanction for unlawful disclosure is detailed at section 19 of the CRCA.

Section 18(2)(a) of CRCA provides HMRC with the lawful authority to make a disclosure of HMRC information where it is for a function of HMRC and does not contravene any restriction imposed by the Commissioners. This enables HMRC to disclose information in order for HMRC to carry out its functions of collecting and managing revenue.

Article 6 (1) (e) of the GDPR allows that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. House of Lords Appointments Commission only uses personal data for the purposes of carrying out the task of vetting nominees for peerages.

Article 6 (1) (a) states that the data subject has given consent to the processing of his or her personal data for one or more specific purposes. House of Lords Appointments Commission obtains the written consent of each individual for whom it carries out vetting.

6. Details about the data sharing

Information identifying the individuals to be checked by HMRC is provided by named contacts in the House of Lords Appointments Commission.

Upon receipt of the information, HMRC will identify the nominee and commission reports on the tax behaviour of such nominees and companies, sole proprietorships or partnerships linked to the applicant where significant control is held. The reports are presented to senior HMRC officials who comprise the checking panel for the purpose of arriving at a risk rating. The checking panel use the behaviours contained within the Annex C – Risk rating matrix as a guide to determine a rating based on the level of potential reputational risk to HMRC and the likely adverse impact on tax compliance should the individual’s tax behaviour become generally known.

The data fields to be shared

House of Lords Appointments Commission to HMRC:

- name
- address
- date of birth

HMRC to House of Lords Appointments Commission:

- rating of low/medium/high – no reasons given for that rating

Source systems

For House of Lords Appointments Commission: data and information provided from the nominee.

For HMRC: data held within HMRC compliance and head of duty systems.

Government security classification

Official sensitive – there is no special category data, sensitive data or criminal offence data being shared.

Method by which data will be transferred under this agreement

Both to and from House of Lords Appointments Commission and HMRC will be via Transport Layer Security email. Ratings are returned on a password protected document. The password is sent by separate email.

Accuracy of the data being shared

Before sharing data both Participants must take all reasonable steps to ensure that the data being shared is both accurate and up to date. The exporting department will ensure that data integrity meets their own department's standards, unless more rigorous or higher standards are set out and agreed at the requirements stage. Participants will notify each other of any inaccuracies of the data as they are identified.

Retention and destruction of data

HMRC

HMRC will hold the data in a restricted access-controlled SharePoint site and will retain the data in line with its policy. Data retention policy is either the standard default standard retention period for HMRC records, which is 6

years plus current, (otherwise known as 6 years + 1), unless there is another clear legal, statutory, regulatory, or business exception in place.

HMRC will delete data received from the House Of Lords Appointments Commission via its O365 process.

House Of Lords Appointments Commission

The House Of Lords Appointments Commission will only hold the information while there is a business need to keep it.

The data held by HMRC is accessed only by those specific personnel who work on peerages and who have BPSS clearance or above. This also includes those involved in tracing work, and report writing, who will have basic security checks or higher. They are also bound by the Official Secrets Act and HMRC Data Security.

House Of Lords Appointments Commission will keep the data disclosed by HMRC confidential and without limiting its legal obligations under Data Protection legislation.

Onward disclosure to third parties

House of Lords Appointments Commission agrees to seek permission from HMRC before any onward disclosure of information to a third party and will only disclose any information if permission is granted. Both parties will only use the data they receive for the purposes that it is provided for: namely, to inform a recommendation about whether a peerage nomination should be supported.

Any individual’s HMRC risk rating of low, medium or high is not shared beyond the members of House Of Lords Appointments Commission, the Director General of the Propriety and Ethics Team (and their private office), the Cabinet Secretary (and their private office) and the Prime Minister (and their private office).

House Of Lords Appointments Commission and HMRC will not onwardly disclose the data to any other parties other than those listed here, including the nominee themselves. House of Lords Appointments Commission undertakes to make sure appropriate arrangements are in place with the people who may have sight of a tax rating to ensure confidentiality of that information. Unauthorised disclosures of information to any third parties not listed within the MoU may be reported to the Information Commissioner and result in the MoU being immediately suspended, until satisfactory safeguards are introduced, or ultimately withdrawn.

7. Role of each participant to the MoU

Role of HMRC:

- identify the appropriate data required from HMRC IT systems/records
- provide the data to Participant 2 in as described transferred by secure Transport Layer Security Email from and to agreed contact points
- only allow access to that data by the team requiring it
- ensure that staff handle this data in line with the approved secure transfer method agreed by both departments and within HMRC data security instructions
- only store the data for as long as there is a business need to do so
- move, process and destroy data securely, for example in line with the principles set out in HM Government Security Policy Framework (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework), issued by the Cabinet Office, when handling, transferring, storing, accessing or destroying information
- comply with the requirements in the Security Policy Framework (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework), and in particular prepare for and respond to Security Incidents and to report any data losses, wrongful disclosures or breaches of security relating to information

Role of the House of Lords Appointments Commission:

- identify the appropriate data required from HMRC
- only use the information for purposes that are in accordance with the legal basis under which it was received
- only hold the data for as long as there is a business need to do so
- ensure that only people who have a genuine business need to see the data will have access to it
- on receipt, store data received securely and in accordance with the prevailing central government standards, for example in secure premises and on secure IT systems
- move, process and destroy data securely, for example in line with the principles set out in HM Government Security Policy Framework (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework), issued by the Cabinet Office, when handling, transferring, storing, accessing or destroying information
- comply with the requirements in the Security Policy Framework (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework), and in particular prepare for and respond to Security Incidents and to report any data losses, wrongful disclosures or breaches of security relating to information

- if Participant 2 adheres to a different set of security standards they must inform HMRC what these standards are and comply with any additional security requirements specified by HMRC
- seek permission from HMRC before onward disclosing information to a third party other than those agreed
- seek permission from HMRC if you are considering offshoring any of the personal data shared under this agreement
- mark information assets with the appropriate government security classification and apply the baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile as set out in Government Security Classifications (https://www.gov.uk/government/publications/government-security-classifications), issued by the Cabinet Office, and as a minimum the top level controls framework – Security Controls Framework to the GSC

8. Monitoring and reviewing and arrangements

This MoU relates to a regular exchange that must be reviewed annually to assess whether the MoU is still accurate and fit for purpose.

Reviews outside of the proposed review period can be called by representatives of either Participant. Any changes needed as a result of that review may be agreed in writing and appended to this document for inclusion at the formal review date.

Technical changes necessary to improve the efficiency of the exchange that do not change the overarching purpose can be made without the requirement to review formerly the MoU during its life cycle but must be incorporated at the formal review stage.

A record of all reviews will be created and retained by each Participant.

9. Assurance arrangements

HMRC has a duty of care to assure any data that is passed on to others. Processes covered by this MoU will be subject to annual reviews, from the date of sign off. HMRC may also choose to introduce ad hoc reviews.

Assurance will be provided by the annual completion of a Certificate of Review and Assurance. The assurance processes should include checking that any information sharing is achieving its objectives (in line with this MoU) and that the security arrangements are appropriate given the risks. House of Lords Appointments Commission agrees to provide HMRC with a signed Certificate of Review and Assurance within the time limits specified upon request. HMRC reserves the right to review the agreed risk management, controls, and governance in respect of this specific agreement.

10. Security

The designated points of contact within each department are responsible for notifying the other Participant in writing in the event of loss or unauthorised disclosures of information within 24 hours of the event.

The designated points of contact will discuss and agree the next steps relating to the incident, taking specialist advice where appropriate. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the information, and notifying the Information Commissioner and the data subjects. The arrangements may vary in each case, depending on the sensitivity of the information and the nature of the loss or unauthorised disclosure.

11. Subject access requests

In the event that a Subject Access Request (SAR) is received by either Participant they will issue a formal response on the information that they hold following their internal procedures for responding to the request within the statutory timescales. There is no statutory requirement to re-direct SARs or provide details of the other Participant in the response.

12. Freedom of Information Act (FOI) 2000

Both Participants are subject to the requirements of the Freedom of Information Act (FoIA) 2000 and shall assist and co-operate with each other to enable each organisation to comply with their information disclosure obligations.

In the event of one participant receiving an FoI request that involves disclosing information that has been provided by the other Participant, the organisation in question will notify the other to allow it the opportunity to make representations on the potential impact of disclosure.

All HMRC FoI requests must be notified to the Central HMRC FOI Team: foi.team@hmrc.gov.uk.

Signatories

This content has been withheld because of exemptions in the Freedom of Information Act 2000.

Annex A – Glossary of terms

Definition	Interpretation
Ad hoc transfer	Defined as being bulk data with a protective marking of restricted or above and the transfer is part of a pilot or project with a definitive end date.
Data controller	Has the meaning set out in Article 4 UK GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the Data Protection Act 2018 applies, the meaning in that part if different.
Data processor	Has the meaning set out in Article 4 UK GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the Data Protection Act 2018 applies, the meaning in that part if different.
Data Protection legislation	Means the General Data Protection Regulation, the UK GDPR, the Data Protection Act 2018 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.

Definition	Interpretation
Direct access	Covers an information sharing instance where the receiving department accesses the information via direct, or browser, access to the source system rather than as an extracted information transfer. This agreement will require specific terms and conditions ensuring that access is appropriate and correctly applied, managed and recorded.
Freedom of Information Act (FOI)	Freedom of Information Act 2000 and any subordinate legislation made under this Act together with any guidance and/or codes of practice issued by the Information Commissioner or Ministry of Justice in relation to such legislation.
Granting access	The governance and authority surrounding the authorisation of a person to have access to a system.
Human Rights Act 1998	An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights. Public authorities like HMRC must follow the Act.
Information Asset Owner (IAO)	Means the individual within a directorate, normally the director, responsible for ensuring that information is handled and managed appropriately.
Law	Means any applicable law, statute, bye-law, regulation, order, regulatory policy, guidance or industry code, rule of court or directives or requirements of any regulatory body, delegated or subordinate legislation or notice of any regulatory body.
Provisioning access	The technical channels through which access is made possible, including the request tools associated with this.
Public sector body	This will generally be an other government department (OGD) but could be another public sector body (such as a local authority). Information sharing with a private sector body with which HMRC has a commercial relationship needs to be covered by a commercial contract, not a MoU.
Regulatory bodies	Means those government departments and regulatory statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate,

Definition	Interpretation
	or influence matters dealt with in this agreement and 'regulatory body' shall be construed accordingly.
Senior Information Risk Owner (SIRO)	Provides high level assurance of compliance with HMRC's Information Asset data protection obligations. HMRC's SIRO is the HMRC Chief Digital and Information Officer, Director of Chief Digital and Information Officer Group.

Annex B – Data protection processor relationships

What are data controllers and processors?

The Data Protection Act 2018 (https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted), which draws on the definitions in Article 4 GDPR, defines these as:

The 'data controller' – a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

The 'data processor' – in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

When processing data there will always be a data controller. This controller can establish a 3rd party relationship to assist in processing their data or process the data themselves. Should the controller establish a data processing relationship, this could take the form of a controller-processor, a controller-controller, or a joint controller relationship. Understanding the different 3rd party relationships and their respective requirements is essential to comply with data protection regulations.

It is important to note that the controller can process data but retain the title of controller. You are called a processor only when you are processing with entirely no qualities of a controller.

In summary, the data controller exercises overall control over the ‘why’ and the ‘how’ of a data processing activity, whilst the processor has no involvement in deciding the why and how.

What are the types of data protection 3rd party relationships?

There are 3 types of relationships between controllers and 3rd parties when carrying out the processing of data:

- controller – processor
- controller – controller
- joint controllers

Where personal data is processed there will always be a ‘controller’ – for example, a person (body/individual) who determines the purpose and means of the processing (Article 4(7)). They may do so alone or jointly with others.

How do I begin to define my processor relationship?

It can be challenging to understand both your role and the role of the party you are processing data with. There are different administrative requirements which need to be complied with depending on which type of relationship it is. Without complying you expose yourself to legal risk.

When assessing whether a party is a processor, data controller or a joint controller, the key question is who is determining the purpose and means of processing? In more user friendly terms, who is it that decides why and how personal data is processed?

How do I identify a data controller?

The term data controller is defined by Article 4 of the GDPR as the body/person which determines the means and purposes of processing, and processor is defined as a person/body who carries out processing on behalf of a controller.

To identify a data controller, consider:

- who establishes the lawful basis for collecting the personal data
- who decides what personal data to collect (for example, content of the data)
- who decides the purpose or purposes the data are to be used for
- who decides which individuals to collect data about
- who makes decisions about whether to disclose the data, and if so, who to
- who reviews and decides whether subject access and other individuals' rights apply (such as applications of exemptions)
- who decides how long the data is kept for and whether to make routine amendments to the data

The above actions are those which would be undertaken by a data controller.

Who is the data controller when an organisation is required by law to process personal data?

When personal data is processed only for the purpose and means for which it is required by legislation to be processed, the person who has the obligation under that legislation to process the data is the controller, regardless of whether they appoint another party to carry out the processing. See s.6(2) of the DPA 2018, which is dealt with in less specific terms in the last part of the definition in Article 4(7) of the GDPR. This provision replicates section 1(4) of the 1998 Act.

Annex C – Risk rating matrix

The behaviour types listed are indicative only and not limited to these areas. Categorisation of an individual does not necessarily mean that HMRC considers the individual to have committed the example behaviour traits listed.

HMRC looks back over the last 5 years and seeks to apply the same objective standard to all candidates irrespective of individual circumstances or the nature or status of their vocation or achievements.

Number	Low – No known tax behaviours considered likely to cause adverse public comment	Medium – Disclosure of tax affairs likely to cause adverse comment	High – Disclosure of tax affairs very likely to cause serious adverse comment	Descript
1	Past history of tax avoidance or evasion that relates to a tax year more than 3 years ago (or a shorter period at the panel's discretion), that has since been fully settled. An open avoidance enquiry for just one year but relating to a period 5 or more years ago. At the Panel's discretion, and in exceptional circumstances, where there is open avoidance that can't currently be settled. In all cases no indication that the individual is engaged in further avoidance or evasion.	Currently has one or more open enquiry into use of avoidance where the customer has the opportunity to settle (unless assessed as low).	Currently has one or more open enquiry into use of avoidance, alongside a recent history of serial avoidance over 3 or more tax years.	Avoidanc

Number	Low – No known tax behaviours considered likely to cause adverse public comment	Medium – Disclosure of tax affairs likely to cause adverse comment	High – Disclosure of tax affairs very likely to cause serious adverse comment	Descript
2	Routine compliance checks, not more detailed investigations. Minor issues. Actively engaging with HMRC.	Currently or recently (closed within the last 3 years) subject to a COP 8 investigation into a serious tax loss and cooperating with HMRC. A lack of active engagement with HMRC in dealing with compliance checks, or other correspondence.	Not cooperating with a COP 8 investigation. Currently or recently (closed within the last 3 years) subject to a COP 9 investigation into serious tax fraud. Subject to a current or recent (closed within the last 10 years) criminal investigation. A historical and repetitive lack of active engagement with HMRC in dealing with compliance checks, or other correspondence.	Compliar checks a engagem with HMF
3	All tax returns and payments up to date or where there are minor debts with active engagement to resolve them.	Outstanding returns, or payment arrears. No active engagement with HMRC to remedy the position.	A history of repeated outstanding returns, or payment arrears. No active engagement with HMRC to remedy the position.	Debt and returns complian

Number	Low – No known tax behaviours considered likely to cause adverse public comment	Medium – Disclosure of tax affairs likely to cause adverse comment	High – Disclosure of tax affairs very likely to cause serious adverse comment	Descript
4	No evidence of deliberate behaviour exhibited.	Deliberate behaviour exhibited. HMRC needs to or has needed to: use a production order/use a tribunal approved information notice/seek daily penalties for non-cooperation.	Currently within HMRC's High Risk Wealthy Programme or High Risk Corporates Programme. Evidence of criminal activity, either current or recent.	Behaviou
5	Straightforward disputes involving technical or novel issues of contention. No evidence of boundary pushing.	Disputes where there is evidence of evasion. Evidence of boundary pushing, which goes beyond acceptable tax planning.	Evidence of offshore evasion. Currently within HMRC's Managing Serious Defaulters Programme, or where the customer has been named on gov.uk following an HMRC intervention.	Tax plann arrangem and evas
6	No involvement in illicit trades.	Not directly involved in illicit trades, but there is evidence to suggest was aware, or known	Direct involvement in illicit trades.	Illicit activ (for exam the commerc importati and/or

Number	Low – No known tax behaviours considered likely to cause adverse public comment	Medium – Disclosure of tax affairs likely to cause adverse comment	High – Disclosure of tax affairs very likely to cause serious adverse comment	Descript
		or should have known of the possibility of such activity within their supply chain and does not take action to minimise it.		distributi counterfe goods)
7	Errors identified that breach compliance with excise or customs legislation. Typically, those errors that are minor or where no attempt made to deliberately mislead or evade customs officials.	Importation of goods requiring an appropriate licence without that licence having been obtained. No steps taken to mislead or evade customs officials. Repeated breaches of excise or customs legislation and failure to correct procedures and processes.	Deliberate attempt to smuggle goods with intent to evade excise and customs duty. Includes seizure of goods, no criminal conviction necessary. Deliberate attempt to smuggle drugs and other goods subject to Prohibitions and Restrictions. Includes seizure of goods, no criminal conviction necessary.	Customs
8	Customs - previous (within last 3	Customs - Current (open) compliance	Customs - Offence (including	Customs Strategic

Number	Low – No known tax behaviours considered likely to cause adverse public comment	Medium – Disclosure of tax affairs likely to cause adverse comment	High – Disclosure of tax affairs very likely to cause serious adverse comment	Descript
	years)/current (open) compliance issues with Strategic Exports and Sanctions and Embargoes – routine compliance issues only.	issues with Strategic Exports and Sanctions and Embargoes [no offence established].	Compound Penalty) for issues with Strategic Exports and Sanctions and Embargoes.	Exports a Sanction
9	Engagements where no employment status issues arise or there are technical disputes about status, including where errors were found but were not careless.	Where there is an open enquiry on Engagement(s) where employment status found to be an issue, deemed careless or deliberate	Engagements involving historical and repeated employment status issues that are the subject of separate enquiries, where errors have been established and there is evidence of deliberate attempt not to comply.	Status
10	Money Laundering regulations - minor errors but no sanctions imposed,	Money Laundering Regulations - errors and penalties imposed but not	Money Laundering Regulations - errors and penalties imposed and	Money launderin regulatio

Number	Low – No known tax behaviours considered likely to cause adverse public comment	Medium – Disclosure of tax affairs likely to cause adverse comment	High – Disclosure of tax affairs very likely to cause serious adverse comment	Descript
	advice letter issued.	published on GOV.UK.	published on GOV.UK.	
11	National Minimum Wage regulations - compliant with NMW regulations, or minor breach.	National Minimum Wage Regulations - failure to pay NMW established and there is evidence of attempts to obstruct officers and/or repeated examples where there has been a refusal to answer any questions, furnish information or produce documents when required to do so. Not published by DBT on GOV.UK.	National Minimum Wage Regulations - Failure to pay NMW established and named by DBT on GOV.UK.	National Minimum Wage
12	Errors in claims that have been rectified.	Overclaimed amount due to error that has not been repaid.	Fraudulent claims and/or evidence Deliberate behaviour.	HMRC administe Covid-19 schemes Coronavi Job Rete Scheme (CJRS), S Employm

Number	Low – No known tax behaviours considered likely to cause adverse public comment	Medium – Disclosure of tax affairs likely to cause adverse comment	High – Disclosure of tax affairs very likely to cause serious adverse comment	Descript
				Income Support Scheme (SEISS), Out to He Out (EOI