Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the storage/processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

The DPO's team is available to assist and advise on completing this template.

The template should be submitted to the DPSIA Committee for their recommendations and approval.

For assistance or to submit a DPIA for approval email IGhelp@ico.org.uk.

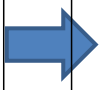
You should start to complete the template as soon as you decide to implement a new system or process. How frequently the DPIA is reviewed and the governance required will vary with the risk of the system or process. At a **minimum**:

Projects: you should produce an initial DPIA prior to finalising your requirements, complete it before finalising your design and review & update the DPIA at least once more prior to go-live. In an Agile project, you should update the DPIA at the start and end of each Epic, or where there is a significant change to the data being processed or the technology or platform. Each update should be submitted to the DPSIA Committee.

Non-projects: you should complete the DPIA prior to designing the service or seeking suppliers and update it whenever there are material changes to the planned system or process.

Screening: Determine what to complete:

1. **GDPR DPIA**: Complete all sections if you meet 2+ questions in section 2.1
2. **Full DPIA**: Complete everything but section 6.2 if you meet 2+ screening questions in any section
3. **Compliance Checklist**: Complete sections 1, 2 and 4, plus signoff, if you don't meet the screening questions



Approval: Consult the DPO's team and select an option for the approvers based on your risk:

1. **DPSIA Committee**: including Senior Information Risk Officer, Head of Cyber Security, DPO
2. **DPSIA Committee**: including DPO and Head of Cyber Security
3. Representatives of DPO and Cyber Security, who will also send it to the DPSIA Committee for their information

Regardless of the option chosen, **the DPIA should be submitted together with your SIA**.

1. Process/system overview

1.1 Summary

Guidance: For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	N/A
Project Title:	Microsoft Cortana Voice Recognition.
Project Manager:	Neil Smithies / Deborah Holt

1.2 Synopsis

Guidance: Provide a summary of the process or system including any relevant background information and the key aims/objectives that the system or process must achieve. There is no need for a detailed discussion of data or data flows – these are covered later in the assessment.

The Microsoft Managed Desktop programme is currently an invite only programme where Microsoft takes responsibility for the configuration, imaging, application deployment, software updates, security and end user support of a device. The service is made up of a combination of existing Microsoft services with an additional monitoring, management and support wrapper.

The components can be summarised as follows;

- Microsoft 365 E5
  - Office 365 E5
  - Windows 10 Enterprise E5
  - Enterprise Mobility + Security E5
- Microsoft Managed Desktop IT as a Service
  - Microsoft Support ("Get Help")
  - Microsoft Operations & Monitoring
- A Microsoft Surface Device

DPSIA's have already been completed for the following areas;

- Office 365 including Enterprise Mobility + Security
- Microsoft Get Help 24x7 Support ("Get Help")
- Microsoft Windows Diagnostics and Telemetry (Advanced Threat Protection)
- Windows Hello Biometric Framework

Scope of this DPSIA

- Microsoft Cortana Voice Recognition

Microsoft provides both a device-based speech recognition feature and a cloud-based (online) speech recognition service.

Turning on the Online speech recognition setting lets you use Microsoft cloud-based speech recognition in Cortana, ~~the Mixed Reality Portal,~~ dictation in

Windows from the software keyboard, supported Microsoft Store apps, and over time, in other parts of Windows.

When you use the Microsoft cloud-based speech recognition service, Microsoft collects and uses your voice recordings to create a text transcription of the spoken words in the voice data. The voice data is used in the aggregate to help improve Microsoft's ability to correctly recognize all users' speech, so the data Microsoft collects from these online services helps to improve them.

You can use device-based speech recognition without sending your voice data to Microsoft. However, the Microsoft cloud-based speech recognition service provides more accurate recognition than the device-based speech recognition. When the Online speech recognition setting is turned off, speech services that don't rely on the cloud and only use device-based recognition—like the Narrator app or the Windows Speech Recognition app—will still work, and Microsoft won't collect any voice data.

If you've given permission in Cortana, we also collect additional information, like your name and nickname, your recent calendar events and the names of the people in your appointments, information about your contacts including names and nicknames, names of your favourite places, apps you use and information about your music preferences. This additional data enables us to better recognise people, events, places and music when you dictate commands, messages or documents.

Online speech recognition is a accessibility feature that allows users to speak to their computer and their speech be represented on screen. This allows speech to text, real time subtitling and real time language translation.

Online speech recognition is turned off by default on an MMD device, however there are not restrictions in place to prevent a user from opting in to this service. At the time of writing, there are no standard management policies available to disable this service completely.

Commented [IEM1]: Can we switch off all of them?

Commented [SJ2]: Which of these things are we actually using / intending to use?

Commented [SJ3]: Most of this is lifted from the Microsoft privacy support documentation but we've omitted the section below. Is there a reason for this? I think it's important that we consider this in the DPIA even if the resulting decision is that we opt to disable this functionality.

If you've allowed Cortana to do so, Microsoft also collects information about your Calendar and People (also known as contacts) to help personalize your speech experience, and to help Windows and Cortana better recognize people, events, places, and music when you dictate messages or documents. The information Cortana collects will help personalize your speech experience on all your Windows devices and Cortana apps when you sign in with the same Microsoft account.

Commented [NS4R3]: I don't think it was on the support document when I stole it.

Commented [SJ5]: So do we want staff to be able to use this functionality or are we happy with it being disabled?

Commented [SJ6]: Most of this is lifted from the Microsoft privacy support documentation but we've omitted the section below. Is there a reason for this? I think it's important that we consider this in the DPIA even if the resulting decision is that we opt to disable this functionality.

If you've allowed Cortana to do so, Microsoft also collects information about your Calendar and People (also known as contacts) to help personalize your speech experience, and to help Windows and Cortana better recognize people, events, places, and music when you dictate messages or documents. The information Cortana collects will help personalize your speech experience on all your Windows devices and Cortana apps when you sign in with the same Microsoft account.

Commented [SJ7]: Potentially calendar and contact information too.

Also if Microsoft collects voice recordings to create a transcript of the spoken words then potentially the personal data shared could be broader. For example if I dictate a letter to a customer about a complaint it will contain that customers personal data – this DPIA needs to consider if we are comfortable with that

Commented [SJ8]: Potentially others depending on what is dictated

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO & Microsoft ~~Michael Fitzgerald~~
Data processor(s)	Microsoft
Purpose of processing	Voice control and dictation
Categories of data	Speech
Categories of subjects	ICO Staff, ICO staff contacts and event organisers, invitees. Subjects of ICO communications depending

	on what is actually dictated
Categories of recipients	Microsoft Speech Recognition Servers and occasionally staff
Overseas transfers	Microsoft staff and speech reconigtion servers are located globally.

1.4 Purpose for processing

Guidance: State the business need being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

~~When you use the Microsoft cloud-based speech recognition service, Microsoft collects and uses your voice recordings to create a text transcription of the spoken words in the voice data. The voice data is used in the aggregate to help improve Microsoft's ability to correctly recognize all users' speech, so the data Microsoft collects from these online services helps to improve them.~~This data is processed if an ICO user wishes to dicate directly to their Windows 10 device, this may be an accessibility requirement, reducing the need for keyboard input or may be a requirement for real time subtliting or translation of streaming video content (such as a staff presentation or briefing)

Commented [SJ9]: This has all already been stated above. This section needs to focus on why we at the ICO want to use these features. What aim is being pursued? Some examples of what we think staff will use this for would be useful.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, protecting the vital interests of a natural person, public task or legitimate interests). If you are processing based on legitimate interests you must also complete a legitimate interests assessment.

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will also need to state a further basis for that processing – you can find a list of these in GDPR Article 9 and 10.

~~User is briefed on speech recognition as part of on-boarding process. Online speech recognition is disabled by default on an MMD device.~~

The lawful basis for processing is Article 6(1)(f) – legitimate interests. For the processing of any special categories of personal data the the lawful basis is Article 9(2) XXXX

Commented [SJ10]: A legitimate interest assessment will be needed

Commented [SJ11]: Need to confirm appropriate lawful basis once we know more about why we want to use this functionality.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

Data Accuracy

a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

Retention & Deletion

d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period
f) Personal data must be erased upon receipt of a lawful request from the data subject

Information & Transparency

g) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected
(iv) Details of the recipients of personal data

Objection & Restriction

h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject

Security

j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
k) Identify an Information Asset Owner
l) Update the Information Asset Register

Is the data being transferred outside the UK and EEA? If so:

m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

Is the data being transferred to or through another organisation? If so:

o) There must be controls to ensure or monitor compliance by external organisations.

Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:

p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject
q) The consent must be recorded in some manner to serve as evidence

Does our Privacy Notice need to be updated? If so:

r) *Update the Privacy Notice*

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	~~N~~Y
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy.	N
9	Does the processing prevent individuals from exercising a	N

Commented [SJ12]: Potentially Yes depending on PD involved

	rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	

Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions please proceed to section 6.

2.2 DPIA approach and consultation

Commented [SJ13]: Needs completion

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Microsoft documentation and privacy policy reviewed, alternate software offerings and costs identified.

Formatted: Font: Not Bold

Review of administrative controls for Speech Recognition in MMD and Intune Portals completed – currently immature. Enhancement request to allow centralised management of Speech Recongition controls in progress with Microsoft.

3. Data inventory

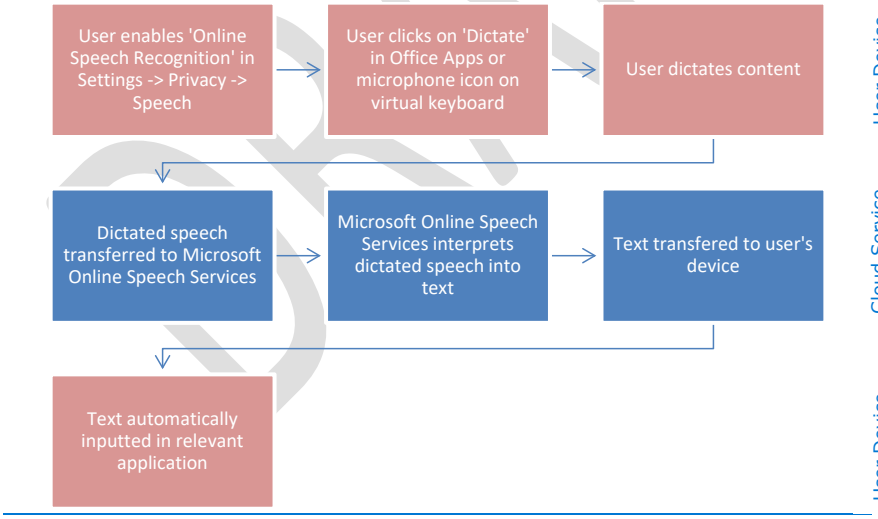
3.1 Information flows

Commented [SJ14]: Needs completing

Guidance: Provide a systematic description of the processing, including:

- *Whether data collected is personal data*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*
- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.



Formatted: Font: 9 pt
Formatted: Centered
Formatted: Centered
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Centered

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	Recipients	Retention Period	Necessity
Speech data (audio recordings) when user opts into to Online speech recognition.	Microsoft speech recognition servers.	Aggregated, anonymised voice data is stored indefinitely unless a user opts to delete records via the Microsoft Privacy Portal.	This is used when a user opts into online speech recognition in order to improve the efficiency of the speech recognition.
Calendar and contact information	Microsoft speech recognition servers.	Aggregated, anonymised voice data is stored indefinitely unless a user opts to delete records via the Microsoft Privacy Portal.	This is used when a user opts into online speech recognition in order to improve the efficiency of the speech recognition.
Personal data / special category data recorded when dictated	Microsoft speech recognition servers.	Aggregated, anonymised voice data is stored indefinitely unless a user opts to delete records via the Microsoft Privacy Portal.	This is used when a user opts into online speech recognition in order to improve the efficiency of the speech recognition.

Commented [IEM15]: Are staff suitably informed about those choices?

Commented [NS16R15]: The information is clear when a user opts to activate the service

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

4. Compliance measures

Use this section to record your compliance with the requirements in section 1.5. Fill in the details of how the requirements have been met or list the requirement as N/A. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	Implementation Details
Data Accuracy	
a) Data must be kept up to date	n/a
b) There must be means to validate the accuracy of any personal data collected	n/a – personal data is not collected as part of this process Personal calendar appointments may be converted to speech by this service. This data is a literal speech conversion of the data that the user has entered into their calender.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	n/a
Retention & Deletion	
d) All data collected will have a retention period	
e) Data must be deleted at the end of its retention period	
f) Personal data must be erased upon receipt of a lawful request from the data subject	Data can be deleted by a user through the Microsoft Privacy Portal.
Information & Transparency	
g) The data subjects shall be provided with: • the identity and contact details of the data controller; • the contact details of the Data Protection Officer; • the purposes of the processing, including the legal basis and legitimate interests pursued • details of the categories of personal data collected • details of the recipients of personal data	Information is provided to users during the device onboarding process
Objection & Restriction	
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	User must 'activate' speech recognition and opt in to online speech recognition.
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject	User must 'activate' speech recognition and opt in to online speech recognition, this can be turned off at any time.
Security	
j) Appropriate training and instructions will be put in place to enable staff to operate the new	~~Information is provided to users during the device onboarding process, ICO staff are available during on boarding to support the process. Microsoft~~

Commented [SJ17]: Need to clarify personal data involved before we can consider comoliance measures and risk assessment

Commented [IEM18]: Not sure this is accurate, voice identification is PD! Also all information on calendar for example hospital appointment etc

Commented [NS19R18]: It's not voice identification as it isn't fingerprinting your voice and using it's unique characteristics to assign an identity to it. It's transcribing your speech which is a different thing.

Commented [IEM20]: Any clear written guifdance about privacy controls, for example switching off cloud recognition or deleting voice data?

system / process securely	~~Windows has detailed instructions to support the user during the process.~~User guidance to be issued on the privacy implications of this service, once a determination has been made over it's appropriateness for the ICO.
k) Identify an Information Asset Owner	IAO is Michael Fitzgerald.
l) Update the Information Asset Register	
Conditional Requirements	
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	Data is covered by Privacy Shield.
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	
o) There must be controls to ensure or monitor compliance by external organisations.	
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	Data can be accessed, downloaded or deleted via the Microsoft Privacy Portal.
q) The consent must be recorded in some manner to serve as evidence	
r) Update the Privacy Notice	

Commented [IEM21]: Is this all covered by privacy shield ?

5. Data protection risk assessment

Guidance: Identify and assess the risks to subjects' rights, the actions you could take to reduce the risks and any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you. This list is not comprehensive and will not necessarily apply to your system or process. See Appendix for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Risk Details	**Impact**	**Probability**	**Response**
[Guidance: Describe risks to data subjects]	*[Guidance: Describe consequences to data subjects if risk realised]*	*[Guidance: Describe likelihood that risk will be realised]*	*[Guidance: Describe risk treatment (eg reduce, avoid, accept or transfer)]*
Processing – A user opts into online speech recognition and dictates confidential information, which cannot be processed by the server and is consequently heard by a Microsoft employee.	Microsoft employee becomes aware of potentially confidential information.	Medium	Accept - Issue guidance that 'online speech recognition' is not suitable for confidential material. Microsoft employees bound by non-disclosure agreements so unlikely that they will act on the information that they receive.
Illegitimate Access to Data – A user opts into online speech recognition	Potentially confidential information is overheard by	Low – Microsoft have access controls in place to prevent this	Accept - Issue guidance that 'online speech recognition' is not

Commented [IEM22]: Has this already been issued?

Commented [IEM23]: What are they?

and a rogue Microsoft employee accesses stored voice recordings.	Microsoft employee	from happening. Microsoft Employees are only given 10 seconds of audio to analyse, audio is analysed in a secure Microsoft facility and association between audio file and a specific user is obfuscated.	suitable for confidential material. Microsoft employees bound by non-disclosure agreements so unlikely that they will act on the information that they receive.

6. Residual risk and sign off

6.1 Residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects. If you have not answered "Yes" to any of the screening questions in Section 2.1 you can leave this section blank.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	[Record any changes recommended by the DPO here]	[Record the actions taken as a result of the recommendation]

6.4 Sign Off

Guidance: Send this to the DPSIA Committee to approve the privacy and security risks involved in the project, the solutions to be implemented and the residual risk.

Approved by	Role	Date	Project Stage
	DPO		
	Head of Cyber Security		
	[Add others as necessary]		

7. Integrate the outcomes back into the plan

Guidance: Who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date

Contact point(s) for future data protection concerns	

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	1.1
Status	Final release
Owner	DPSIA Committee
Release date	02/04/19
Review date	10/12/20

Appendix: Risk Assessment Criteria
The following criteria are aligned with our corporate risk assessment criteria.

Impact
Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.