Data Protection Impact Assessment – Onboarding Checks at Case Officer Assessment Centres

Document Name	Data Protection Impact Assessment – Onboarding Checks at Case Officer Assessment Centres
Author/Owner (name and job title)	Rosie Hunt, HR Manager
Department/Team	People Services
Document Status (draft, published or superseded)	Published
Version Number	V1.0
Release Date	09/08/2023
Approver (if applicable)	Sara Lal, Director of People
Review Date	09/08/2024
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to our privacy by design process. You should use this every time you want to implement or change a product or process at the ICO. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

- It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

- Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting and why, where it will be stored, for how long will you keep it, who will access it and for what purpose, how it will be kept secure and whether it's being transferred to any other country.

- Your Information Asset Owner (your Service Director) is ultimately responsible for managing any residual risk.

- The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

- You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks resulting from what you're proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

- You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

- You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If that's the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The DPIA process

- You should review our internal DPIA Process and allow time for this process in your project plans. Start early! How long it takes will depend on what you're proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Guidance for completing this template – please read.

- You only need to complete this Data Protection Impact Assessment (DPIA) template if you have completed a Screening assessment - do I need to do a DPIA?
- If you're unsure whether you need to complete a DPIA use the screening assessment first to help you decide.
- Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.
- Guidance notes are included within this template to help you – just hover your mouse over any blue text for further information. In some sections links are provided to ICO guidance for further information.
- It is recommended that you fill out each section of this template in order as each subsequent section builds upon the last. You will not be able to complete later sections correctly if you skip ahead.
- If you are struggling with any sections of this template the Information Management and Compliance Service is available to provide advice and support. Please keep in mind their service standards if you require help.

1. Process/system overview

1.1 Ownership

Guidance Link: Controllers and processors | ICO

Project Title:	Onboarding Checks at Case Officer Assessment Centres
Project Manager:	Rosie Hunt, HR Manager
Information Asset Owner:	Sarah Lal, Director People Services
Controller(s)	ICO
Data processor(s)	N/A

1.2 Describe your new service or process

Discussions have been taking place within the People Services Directorate regarding how we can accommodate a seamless onboarding process for large scale recruitment campaigns such as Case Officer assessment centres.

For such campaigns, it suits the business to have a large number of starters join as quickly as possible, ideally on the same day. An obstacle to this in the past has been the time it takes for pre-employment checks to be completed, specifically, the time it takes for HR to obtain documents needed from the candidates to process their DBS/ID/right to work checks/qualification checks. For these checks, we must see physical original documents – so candidates have to attend our Wilmslow office in person or post them to us if it is not practical for them to attend the office.

Assessment Centres will always take place at our offices in Wilmslow.

Potential solution:

Ask those attending the assessment centre to pre-prepare the necessary personal documents that would be required to process their pre-employment checks, and to bring this with them on the day of their assessment centre.

A member of HR would be present on the day of the assessment centre to see the physical documents and take photocopies or digital scans, and confirm likeness of the individual against any photo ID provided (ahead of job offers being made). This will allow HR to start processing the necessary checks immediately once a job offer is accepted rather than waiting potentially weeks after the offer being made for the physical documents to be provided.

It also creates a more streamlined experience for the successful candidates as they would not be required to attend the office again to provide the documents at a later date (this is often a challenge as individuals struggle to get the time off work during business hours to attend the office).

Collating the documents in advance of an offer allows us to be ready and react immediately once an offer is accepted.

It is common practice across the recruitment sector for such documents to be collated in advance of an offer being made, so the relevant checks can proceed immediately once an offer is accepted. This approach is also adopted by the Government Recruitment Service and we've also had conversations with contacts at the Cabinet Office who've confirmed this is the approach they take with their recruitment campaigns. Similarly People Services colleagues who have recently joined the ICO from the private sector have experience of this approach being adopted widely across the recruitment sector.

The scope of this DPIA is the ICOs collection and storage of the information required to complete pre-employment checks. The significant change to existing practices will be the collection of this data about *all* candidates applying to ICO roles, as opposed to the current process where this data is only collected from *successful* candidates after they have been deemed appointable and accepted a role. This approach will only be taken for assessment centre recruitment campaigns where we anticipate recruiting multiple candidates for a role.

1.3 Personal data inventory - explain what personal data is involved

Guidance Link: What is personal data? | ICO

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
ID documents, for the purposes of processing identity, right to work, and DBS checks. Examples include, but are not limited to passport, driver's license, birth/adoption certificate, marriage/civil partnership certificate, mortgage statement, bank statement, council tax statement, p45/p60. At least one of the documents provided is likely to be special category data. The full list of documents we're able to accept for right to work is in section 7 here: An employer's guide to right to work checks: 6 April 2022 (accessible version) - GOV.UK (www.gov.uk)	Candidate	HR	N/A	Unsuccessful candidates: destroy immediately Reserve list candidates: 6 months. Successful candidates: End of employment + 2 years.

For DBS checks see Pre-employment checking - document requirements. The candidate provides 1 document from Group 1, and 2 further documents from either Group 1, 2a, or 2b.				
Educational certificates as evidence of qualifications that are a requirement for the job role.	Candidate	HR	N/A	Unsuccessful candidates: destroy immediately Reserve list candidates: 6 months. Successful candidates: End of employment + 2 years

1.4 Identify a lawful basis for your processing

Guidance Link: Lawful basis for processing & Lawful basis interactive guidance tool

The collection and storage of personal data about all candidates at the assessment centre stage of our recruitment process is carried out under the legitimate interests lawful basis – Article 6(1)(f).

We have a legitimate interest in ensuring our recruitment processes are as efficient as possible so we can ensure we minimise any delay to successful candidates being able to commence their role at the ICO once they have accepted a job offer. Delays to the recruitment of candidates can have a significant impact on the delivery of key services to our customers. Delays also affect the individual employee as they are unable to start their role at the ICO. Often they won't be earning an income whilst they await their start date and this can impact on their personal finances.

Due to the potential processing of marriage / civil partnership certificates as a form of ID special category data may be processed. The relevant processing conditions are Article 9(2)(g) – necessary for reasons of substantial public interest. And schedule 1, part 2 paragraph 6 – statutory etc and government purposes.

It is worth noting that for successful candidates whose documents are then processed for right to work and identity checks the lawful basis for this further processing will be:

Right to work checks – Article 6(1)(c) - legal obligation.

Identity checks, DBS checks, Educational certificates – Article 6(1)(b) necessary for the performance of a contract.

Due to the potential processing of marriage / civil partnership certificates as a form of ID special category data may be processed. The relevant processing conditions are Article 9(2)(b) – employment and Schedule 1 Part 1 paragraph 1 of the DPA 2018.

1.5 Explain why it is both necessary and proportionate to process the personal data you've listed in your data inventory

The type of personal data being processed is not changing. It is the point at which we start processing it (collating it), before an offer of employment is made.

It is necessary and proportionate to obtain this data at interview in order to streamline the onboarding process for both the candidate and the business (see page 5 for some further details).

We currently utilise assessment centres to recruit multiple candidates for the same role in order to address significant shortfalls in staff numbers in the recruiting departments. Candidates attending assessment centres have already passed the application stage of our recruitment process, and have therefore already been assessed as having the potential for appointment.

Due to the volume of successful candidates that we typically recruit from an assessment centre delays to employee start dates can adversely impact the business and the services we're able to deliver to our customers.

These impacts can include;

- HR Assistants spending a considerable amount of time scheduling individual appointments with prospective employees for them to attend the office to provide their documents. The change in process would reduce the need for us to contact individual candidates, arrange appointments and have a member of the HR Team attend the office on the days that are convenient for all parties to take copies of the necessary documents.
- Recruiting departments experience delays in their new employees starting their roles; this impacts on their ability to deliver their services to our customers. Employees can't start until the necessary checks have been completed and delays at the stage of document provision by candidates mean delays to start dates.
- New starters typically require a significant amount of training before they can work independently in their role. It takes a considerable effort to coordinate training for a number of new starters and it is more efficient to deliver training to all new employees as a single cohort. Delays in start dates whilst we wait for pre-employment checks to be completed can result in us having to stagger training modules for different employees depending on their start date. This has a considerable impact on all colleagues involved in the training process and can result in us having to run multiple training sessions as opposed to one session for all new employees. This means more admin and training hours that could be avoided by this change in process.
- Delays to employee start dates resulting in loss of income for data subjects.

For successful candidates they will have to provide the necessary documentation for the pre-employment checks at some point prior to employment. There is therefore little impact to them from the ICO collecting this at an earlier stage of the process, and we have existing controls to ensure that this data is kept safe and secure.

For candidates that are ultimately unsuccessful at the assessment centre they will have provided us with their documents, yet we won't need to further process them beyond the initial collection and storage. We intend to put in place robust processes to ensure that these documents are securely deleted and not retained by the ICO for longer than is necessary. Again there is limited impact on the individuals as a result of the ICO collecting and storing their documents for the limited period of time between the date of the assessment centre and the notification of the outcomes.

Should candidates fail to provide their documentation at the assessment centre stage there will be no prejudice or detriment to them. If they are appointable and accept a role we would simply revert to the existing process and arrange for them to attend the office to provide the necessary documents.

The risk assessment below provides further detail about likelihood and severity of any impact on data subjects as a result of this change in process and there are clear benefits to be gained for the ICO, our customers and the data subjects involved if we adopt the proposed change. There is no other way we can achieve our objectives and the collection of the personal data is considered proportionate to achieve the desired outcome.

1.6 Outline your approach to completing this DPIA

This proposed approach was first discussed between HR and Talent Teams.

I consulted the Information Management Team informally in the first instance by email outlining this proposal, and was subsequently asked to complete this DPIA to provide further detail due to fact it involves special category data.

I have consulted the ICO website to determine the lawful basis for processing.

2.0 Personal Data Lifecycle

Guidance Note:

- You must provide a systematic description of your processing from the point that personal data is first collected through to its disposal.
- You should explain the source of the data, how it is obtained, what technology is used to process is, who has access to it, where it is stored and how and when it is disposed of.
- If your plans involve the use of any new technology, you should explain how this technology works and outline any 'privacy friendly' features that are available.

- You can use the headings provided below to help you construct your lifecycle. Also include a flow diagram if it helps your explanation.

Data source and collection:

The ID documents and certificates would be provided by the candidate at the Assessment Centre. The Assessment Centre will take place at the Wilmslow Office. The documents will be received by HR, and copies taken.

Technology used for the processing:

A scan of the documents will be taken.

Storage location:

Documents will be scanned to negate the need for hard photocopies to be stored. Scanned documents will be stored in a central folder within HR's SharePoint area. The person who has scanned the copy will ensure that the emailed copy is deleted from their inbox.

Access controls and data sharing:

Only the relevant members of the HR Team will have access to the documents, i.e., those responsible for processing pre-employment checks. These will not be shared more widely.

Disposal:

For unsuccessful candidates, scanned documents will be destroyed within 2 weeks of the assessment centre taking place. For candidates on a reserve list, we would like to hold the documents for 6 months on the basis that they may be offered a role during this time. For successful candidates, the documents will be held on their employment file for the end of employment + 2 years.

The HR Assistants are responsible for onboarding and will hold responsibility for scanning documents at Assessment Centres, thus they will hold responsibility for the timely disposal of documents.

The HR Assistant will diarise a reminder to delete the documents of unsuccessful candidates 2 weeks from the Assessment Centre has taken place. Documents may well have been deleted before this if we receive outcomes from hiring managers sooner, but this reminder will act as an extra measure to delete/check if documents have indeed been deleted.

For candidates on reserve lists, we will diarise a reminder 6 months from the date of the Assessment Centre for all remaining documents held to be deleted.

3.0 Key GDPR principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☒ No ☐

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Guidance Link: Consent

Yes ☐ No ☐ N/a ☒

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☒ N/a ☐

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

The personal data held by the ICO will be an accurate copy (digital scan) of the information provided to us by the data subject and should not need to change during the time that the ICO processes it.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

N/A

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

HR will set calendar reminders – please see page 9 for further details.

10. Will you need to update the retention and disposal schedule?

Yes ☒ No ☐

Integrity and confidentiality

11. Where will the personal data be stored?

Scanned copies will be stored electronically within HR's SharePoint area. No hard copies will be stored.

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☐ No ☐ N/a ☒

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

We would create a new checklist to be used for Case Officer Assessment Centres which would detail the exact tasks to be undertaken in relation to this new process.

As it is a new process, training will be given to staff involved on what the process entails and the importance, timing and methods of disposing of documents where candidates are unsuccessful. This will also involve familiarising them with the new checklist.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Sarah Lal, Director of People Services

16. Will you need to update our Article 30 record of processing activities?

Yes ☐ No ☒

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☐ No ☐ N/a ☒

Individual Rights

Guidance Note:

- UK GDPR provides a number of rights to data subjects where their personal data is being processed.
- As some rights are not absolute and only apply in limited circumstances we may have grounds to refuse a specific request from an individual data subject. But you need to be sure your new service or process can facilitate the exercise of these rights and it should be technically feasible for us to action a request if required.

Guidance Link: Individual rights

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☐ No ☐ N/a ☒

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

Risk Description		Response to Risk	Risk Mitigation	Expected Risk Score		
				I	P	Total
				See Appendix 1 – Risk Assessment Criteria		
Example: *Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.*		*Reduce*	*Existing mitigation: We have checked that the system we intend to procure allows us to set access permissions for different users.* *Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.*	*3*	*1*	*3 - low*
1.	Documents are unnecessarily retained for unsuccessful candidates	Reduce	Expected Mitigation: We will add it into HR process checklists, that when receiving the outcomes of an assessment centre, the documents belonging to the unsuccessful candidates are deleted immediately.	3	1	3 - low
2.	Documents are unnecessarily retained for reserve list candidates	Reduce	Expected Mitigation We will add it into HR process checklists, that when receiving the outcomes of an assessment centre, we set a calendar reminder to delete the documents for any	3	1	3 - low

			candidates who were placed on a reserve list and have not been appointed.			
3.	Candidates experience bias or discrimination as a result of providing data at an early stage	Accept	Existing Mitigation Recruitment decisions are made by the recruiting managers rather than the HR staff involved in the process of collection and storage of documents required for ID purposes. Recruiting managers don't have site of these documents so decisions about the candidates competency for the role can't be influenced by the provision of these documents at an earlier stage.	4	1	4 - low
4.	Excessive collection of personal data	Accept	Existing Mitigation: Steps have been taken to consider the necessity and proportionality of the data collection as part of this DPIA. There is a demonstrable legitimate interest in the ICO collecting this personal data at the proposed stage of the recruitment process and we'll only be collecting what is necessary for pre-employment checks should an applicant be successful. The data collection is justifiable and is not considered to be excessive. The legitimate interest being pursued can only be achieved by the collection of this data.	2	2	4 - low

5.0 Consult the DPO

Guidance Note:

- Once you have completed all of the sections above you should submit your DPIA for consideration by the DPIA Forum who will provide you with recommendations on behalf of our Data Protection Officer (DPO). The process to follow is here.

- Any recommendations from the DPOs team will be recorded below and your DPIA will then be returned to you. You must then record your response to each recommendation and proceed with the rest of the template.

	Recommendation	**Date and project stage**	**Project Team Response**
1.	When reviewing the Home Office guidance for right to work checks (RTW) it was noted that validity checks on identity documents must take place in the presence of the applicant. If these are intended to take place on the day of the assessment centre, does this mean you will actually be completing RTW checks on all applicants not just those who are successful at the assessment centre? Please can you clarify this and update the DPIA accordingly as it's unclear whether you're just taking scans with the intention to complete checks at a	Planning 14/04/2023	The right to work check is one check of several mentioned earlier in this document that form part of the onboarding process. The appointed member of HR present on the day would take a photocopy of the documents (including evidence of right to work) and at this point confirm likeness of any photo ID to that of the individual presenting it and confirm that originals have been presented. This is as far as any of the checks would go at this point. If the candidate was successful, we would confirm whether the photocopy provides sufficient evidence of the individual's right to work, and the evidence would be filed on the personal file, and the remaining checks would be processed using the copies of original documents that had been taken at the assessment centre.

	later date for successful applicants (which may require them to return to the office) or if RTW check will be carried out for all applicants on the day of the assessment centre.		There would be no requirement for the individual to attend the office again in person providing the necessary original documents were produced at the assessment centre – as the original would have been seen, and personal likeness against any photo ID confirmed.
2.	The Home Office guidance also indicates that copies of the documents should be retained for 2 years after the employee ceases working for the ICO yet our current practice is to retain these for 6 months from the end of employment. In light of the HO guidance we'd recommend a change of practice to reflect the updated HO position and the Information Management and Compliance Service will update the ICO retention schedule. In this DPIA references to end of employment plus 6 months should be replaced with end of employment plus 2 years.	Planning 14/04/2023	Our dedicated LIMO has been informed, the Team has been updated, and our retention schedule has been updated to reflect this recommended change in practice. Any references that previously existed within this document to end of employment plus 6 months have been updated to end of employment plus 2 years.

6.0 Integrate the DPIA outcomes back into your plans

Guidance Note:

- Completing sections 1 to 5 of your DPIA should have helped you identify a number of key actions that you now need to take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement.

- You should also consider whether any additional actions are required as a result of any recommendations you received from the DPO.

- Use the table below to list the actions you need to take and track your progress with implementation. Most actions will typically need to be completed *before* you can start your processing.

Action	**Date for completion**	**Responsibility for Action**	**Completed Date**
Update retention schedule	ASAP	IMC Service	14/04/2023
Update Privacy Notice	Before implementation	IMC Service / Rosie Hunt HR Manager	28/06/2023
Update HR process checklists and train HR staff on new retention and disposal requirements; importance, timing and methods of disposing of documents where candidates are unsuccessful.	Before implementation	Rosie Hunt, HR Manager	01/08/2023

7.0 Expected residual risk and sign off by IAO

Guidance note:

- Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk ***after*** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.
- If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

Residual risk is deemed low.

We have a robust process in place supported by a checklist to ensure that all steps within the personal data lifecycle (outlined earlier in this document) are followed.

The risk is that we hold personal data for unsuccessful candidates for longer than necessary. I deem this to be low risk, on the basis that the Team are fully acquainted with carrying out these checks, and the importance of completing the associated checklist.

7.1 IAO sign off

Guidance Note:

- Your IAO owns the risks associated with your processing and they have final sign off on your plans. You **must** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.

IAO (name and role)	Date of sign off
Sarah Lal, Director of People	09 August 2023

8.0 DPIA Change history

Version	Date	Author	Change description
V0.1	February 2023	Rosie Hunt	First Draft
V0.1	14/04/2023	Steven Johnston	DPO recommendations added to 5.0. Actions updated and IMC actions completed.

V1.0	09/08/2023	Rosie Hunt / Sarah Lal	IAO Sign off and first release.

Appendix 1: 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.

Appendix 2: example risks to data subjects

Guidance Note:

- The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles