

DWP Data Protection Impact Assessment

Part 2 – detailed assessment

About the detailed assessment

Only complete this detailed assessment when instructed to do so by the Data Protection Officer's (DPO) team after submitting a DPIA part 1: screening assessment.

When completing this form use plain, simple language. Avoid jargon and write out acronyms. This will prevent us having to ask you for explanations.

The detailed assessment consists of three sections:

- Section 1: The nature, scope, context and purpose of the processing
- Section 2: Identification, assessment and mitigation of risks
- Section 3: Sign off

First, complete section 1. You may not know the precise details of what you are doing, but provide as much information as you can.

Do not complete sections 2 or 3 yet.

Send the form to the DPO team.

The DPO team will work with you to go through the information in section 1. They will help you understand what you need to do.

As you work through the detail of your initiative you will identify risks to individuals. The DPO team will help you complete section 2.

The DPO team will tell you when to complete section 3 to ensure your Senior Responsible Owner (SRO) understands what they need to do.

Where to find more information

The Data Protection by Design guide will help you understand what you need to do. It provides detailed guidance for initiatives on various aspects of data protection.

stated 'The Department has detected around 100,000 claims where it suspects an advance has been applied for fraudulently, worth an estimated £98 million to £147 million. The number of cases of suspected advances fraud continued to grow through the summer of 2019. By the end of December 2019, the Department had identified 97,780 suspected cases of advances fraud. To estimate the level of financial risk it might be exposed to, for internal purposes, the Department has used figures of both £1,000 and £1,500 for an average advances claim. By applying these figures to the 97,780 cases of suspected advances fraud, between £98 million and £147 million of advances claims were potentially fraudulent.'

Advances Model

[REDACTED] will have the ability [REDACTED] to detect UC Advances Fraud.

The Advances model has previous been trained on older UC claims that a fraud investigator has already determined was or was not Advances Fraud. [REDACTED]

[REDACTED]

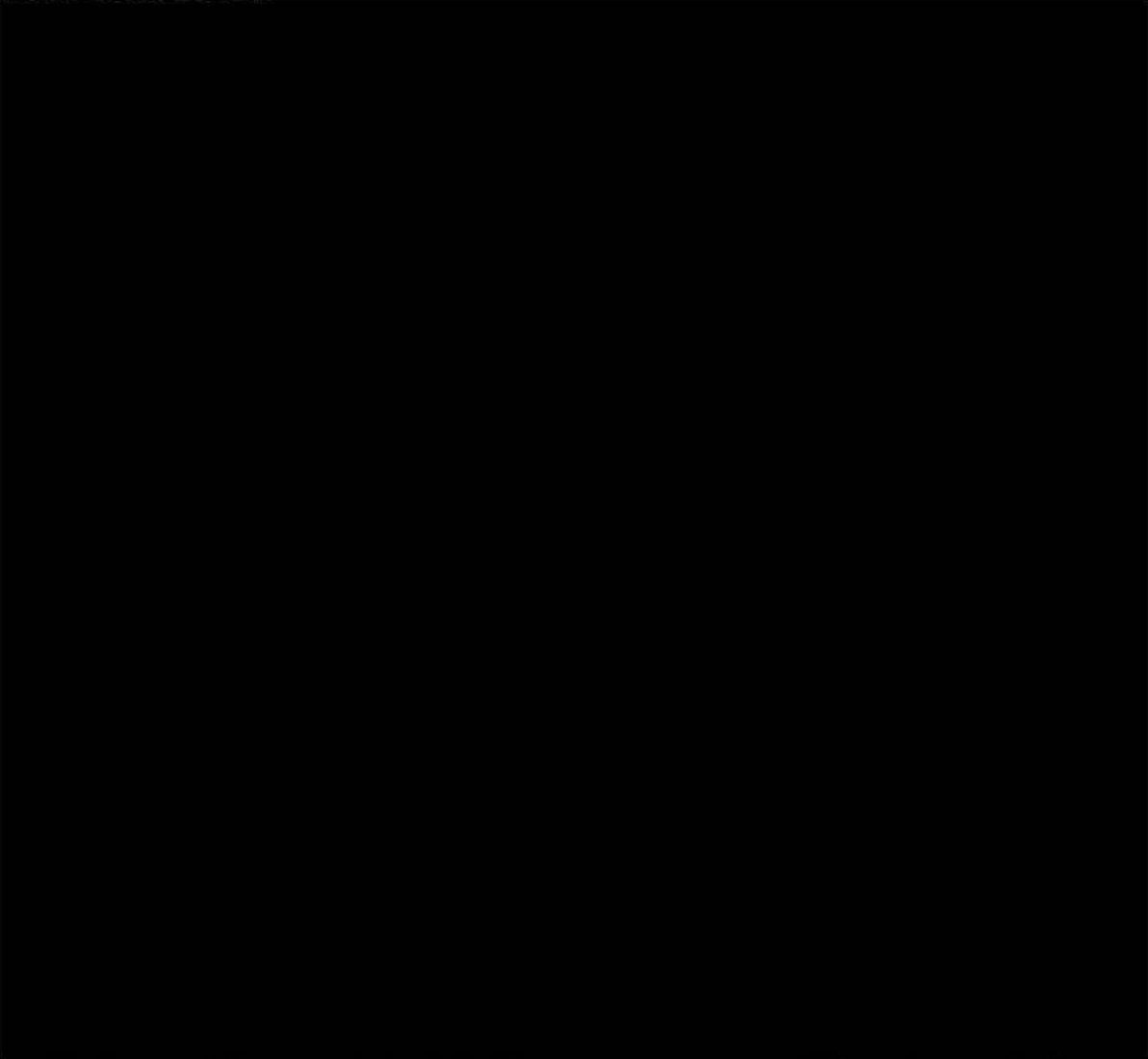
About the personal data and the processing

2. List the personal data items you will be processing for your initiative.

Highlight any data items that are special category data. This means personal data about:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data for the purpose of uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation.

Advances Model



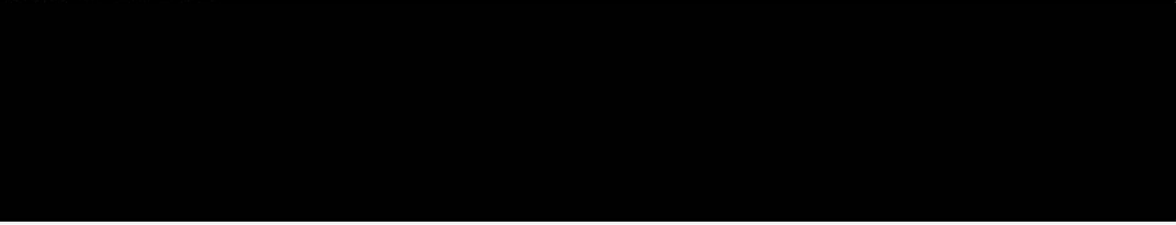
As the model is maintained the inputs may change. If there is a material difference the DPIA will be updated.

3. Specify the source of the personal data.

For example, directly from the individual, other organisations, existing DWP records.

If the data comes from existing DWP records, specify the system that holds the records.

If you obtain personal data from multiple sources, list all of them and state what data will be obtained from each source.



4. Explain how you will obtain the data.

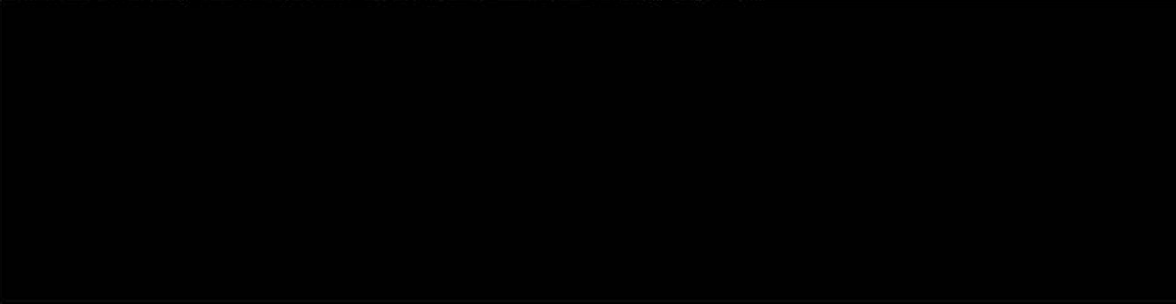
For example, paper form, digital form, face to face, email, electronic transfer, over the telephone.

If there are multiple methods for obtaining data, list all of them and state what data will be collected by each method.



5. Explain how the personal data will be held and what security measures will be in place

Summarise any advice you have received from security experts.



6. List any organisations other than DWP that will be involved in processing the personal data.

In each case explain:

- the role of the organisation in processing the data
- the nature of the relationship to DWP
- what data will be processed, how and why
- how you will ensure organisations will only use the data for the specified purpose
- how the data will be accessed or transferred

- what security measures will be in place.

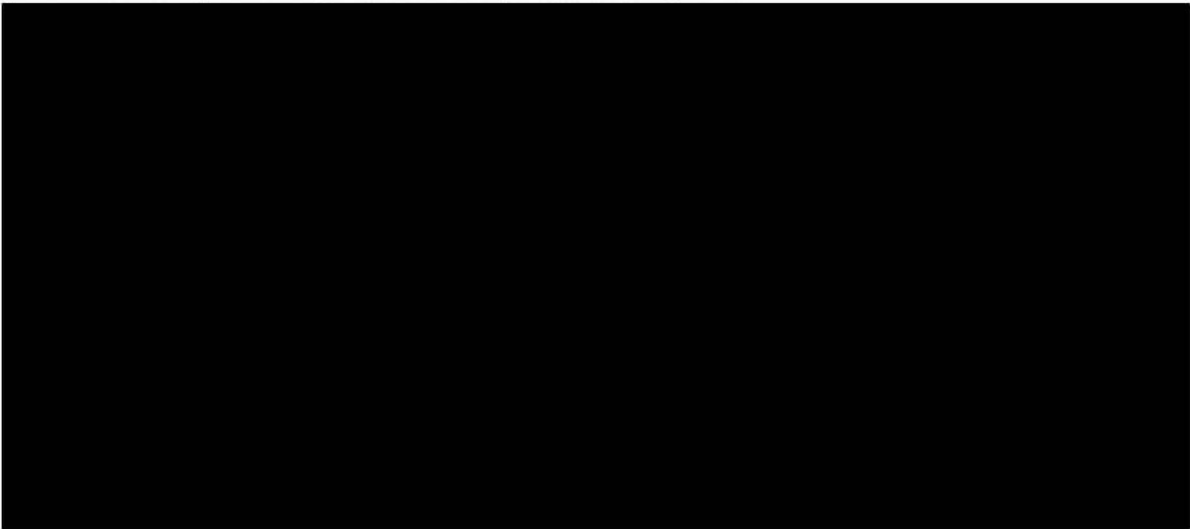
Attach data flow diagrams if necessary.

N/A

7. Specify how long the personal data will be kept and how you will ensure it is not kept for longer.

Include details of how data will be destroyed when they are no longer needed.

Information Management Policy published by DPO will be followed to comply with the GDPR and retention periods will be followed as per the **Retention specific guidelines** published by DPO



8. Explain any processing of personal data that will take place outside the United Kingdom.

This includes any "offshoring" by service providers.

No data processing will take place outside the UK.

9. Explain any processing of personal data using tracking pixels and other types of web beacons, cookies, or similar technology.

Not all cookies or web beacons process personal data.

In most cases IP addresses are personal data. If you will collect IP addresses explain how and why.

There will be no processing of personal data using pixels and other types of web beacon, cookies, or similar technology.

About necessity, proportionality, lawfulness and data quality

10. Explain how processing the personal data listed in question 2 will help achieve your aims

[REDACTED]

Where these appear to be the result of fraud or erro

This may result in either an improvement to future fraud prevention/detection controls, a specific intervention, a policy improvement or all three.

The Common Risk Engine [REDACTED] component of Common Risk Engine (CRE) pulls data from [REDACTED]

[REDACTED] to enable the operational staff within UCFS [REDACTED] to prioritise the review and processing of these claims.

[REDACTED]

The Advances model has previous been trained on older UC claims that a fraud investigator has already determined was or was not Advances Fraud

[REDACTED]

11. Describe any ways of achieving the initiative's aims you have considered that use less or no personal data and explain why you have not pursued them.

The Advances model is trained on personal data of previous UC claims, [REDACTED]

12. Explain how you will ensure that the personal data is of a sufficient quality.

Advances Model

Data will be provided on a transactional basis [REDACTED]

[REDACTED] There will be data stored as part of each of these transactions to allow for continual monitoring of performance metrics and audit purposes. [REDACTED]

13. Specify the lawful basis for processing the personal data.

If you're not sure read the [guidance on the intranet](#). If you are also processing special category data you will need to state two legal bases.

Advances Model

IRIS will use the existing data sources [REDACTED]

GDPR Art 6(1)(e) allows DWP to process data as it is necessary for the performance of a task carried out in the public interest. 'Individuals' may include other people whose data you are processing besides the customer themselves. For example, spouses, children, other people in the household, the cared-for person.

The lawful basis for processing special category data is Article 9(b) Employment, Social Security and Social Protection.

The impact on individuals and their rights

'Individuals' may include other people whose data you are processing besides the customer themselves. For example, spouses, children, other people in the household, the cared-for person.

14. Describe the effect the initiative is intended to have on individuals.

Common Risk Engine - [REDACTED]

[REDACTED] It will enable improved monitoring and audit controls, which in turn, supports the delivery of reductions in Fraud and Error payments.

Before Covid-19, 100% of advances required a Face-to-Face (F2F) UC caseworker intervention. During Covid-19, there was an identified spike in advances fraud due to the lack of F2F caseworker interventions. [REDACTED]

Advances Model

[REDACTED] Our aim is to prevent human bias or reliance on the model as much as possible. [REDACTED]

15. Explain how individuals will know that their personal data will be processed in this way.

If you think the processing is covered by DWP's Personal Information Charter, specify what parts cover it.

Individuals will know how their data is processed through references to DWP's personal information charter on letters issued by Service Delivery Centres, system generated letters or by accessing the Digital front-end systems. Specific information on how we use data is also covered in DWP's Personal Information charter under the following sections:

- What DWP uses personal information for;
- How DWP shares information about you;
- DWP uses of profiling

16. Explain what choice, if any, individuals have about:

- their involvement in the initiative
- how their data are processed.

Claimants (Citizens) do not have a choice on how we process their data for Fraud and Error.

17. Describe any consultation with individuals about the processing of personal data in your initiative that has taken place or is planned

If you do not consider consultation to be necessary, explain why.

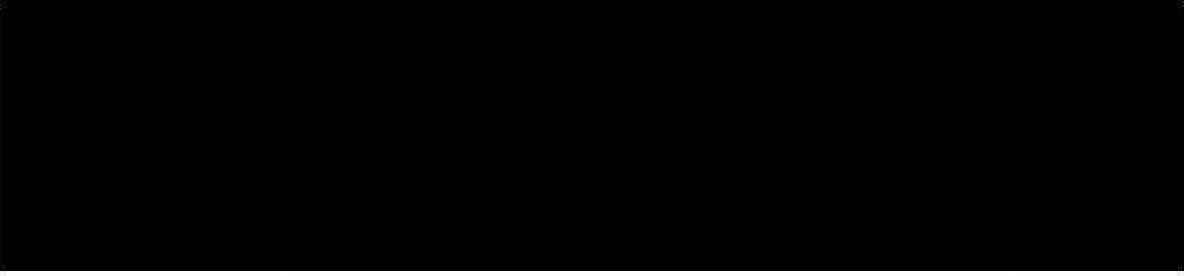
Disclosing information on specific Fraud and Error initiatives, by default, reveals how we are preventing and detecting fraud/error within our benefit system. We would run the risk of providing information that would help fraudsters and those intent on committing crime to know what data, controls and systems DWP has in place to prevent and detect fraud.

18. The right of access: Explain how individuals will be able to access their personal data that will be processed.

In this circumstance a Right of Access Request (RAR) will be raised in name of the system, the Central RAR team (rightofaccess.requests@dwp.gov.uk) will be informed of the details. All information (if required) will be given as per the **Personal Information Charter** and according to **DWP's policy of RARS**.

19. The right to rectification: Explain how the personal data will be updated if an individual informs you that the personal data you hold about them are incorrect or incomplete.

Consider how you will ensure that **all** instances of the data can be identified and updated if required.



All wider data rectification processing will be carried out in line with **DWP GDPR standard policy**.

20. The right to erasure: Explain how you will erase the personal data of an individual if required to do so before the normal retention period.

Consider how you will ensure that all instances of the data can be identified and erased if required. Erasure of data of an individual before a normal retention period can be done at source by Data owners or by [REDACTED] by deleting records used in the analysis of detecting fraud, error or debt. This is in line with **DWP GDPR standard policy**.

21. The right to restrict processing: Explain how you will prevent the personal data of an individual from being erased according to the normal retention period if required to do so.

Consider how you will ensure that all instances of the data can be identified and prevented from being erased if required.

Our workstream does not have access to source data to erase any personal data outside a normal retention period. This would be processed by the owning business unit in accordance with DWP laid down policies.

Automated decision making

Only complete this section if your initiative involves automated decision making.

Automated decisions are those which:

- Are based **solely** on automated processing with no human involvement; **and**
- Have a legal or similarly **significant effect** on the individual

22. Explain the process which leads to the decision.

Advances Model

We do not believe that this process is a 'automated decision' as there is significant human involvement. Any referral is first assessed by a human being. They must determine the outcome. We will collect all results for future iterations of the model to help us refine it. [REDACTED]

[REDACTED] Our model will not be the only thing that effects the processing of an advance. It will simply be an extra thing [REDACTED] to check.

23. Describe the decision and its impact on the individual.

See answer to question 22

24. Explain how people are notified that an automated decision has been made.

See answer to question 22

25. Explain how you will handle requests from individuals to have decisions made by automated means looked at again by human beings.

See answer to question 22

Profiling

Only complete this section if your initiative involves profiling.

'Profiling' means evaluating or scoring individuals using automated processes to analyse or predict aspects about their:

- performance at work;
- economic situation;
- health;
- personal preferences or interests;
- reliability or behaviour;
- location or movements?

26. Specify what aspects of people's lives, characteristics or behaviour you will be predicting or analysing.

Advances Model

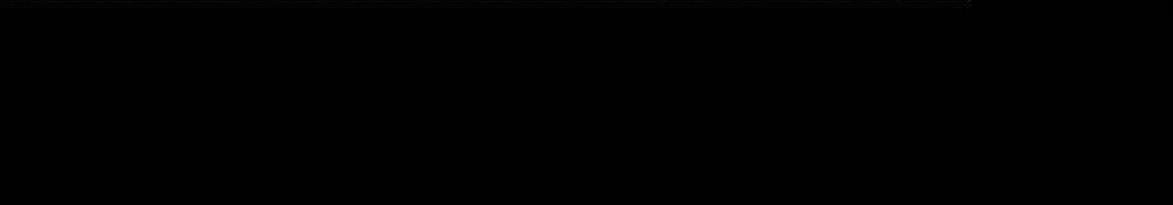
The Advances model has previously been trained on older UC claims that a fraud investigator has already determined was or was not Advances Fraud.



27. Explain why you will be doing this prediction or analysis.

Advance Model

Before Covid-19, 100% of advances required a Face-to-Face (F2F) UC caseworker intervention. During Covid-19, there was an identified spike in advances fraud due to the lack of F2F caseworker interventions.



28. Describe what will happen to individuals as a result of those predictions or that analysis.

Advances Model

The outcome of the analysis will identify service improvements to the Digital

front-end system and knowledge management as well as avoiding unnecessary over or underpayments. This will help to optimise the claimants end to end journey whilst making a claim or reporting a change of circumstances

Significant levels of testing were completed to ensure the impact of the Advances Model outcomes would not have significant adverse impacts on individuals. This involved the training of the model [REDACTED] then getting these outcomes validated [REDACTED]. This testing allowed improvements to the model to minimise bias where possible within the model.

If a UC claim advance is deemed to be potentially fraudulent the impact will be [REDACTED]

Additionally, IRIS [REDACTED] deploy techniques to ensure that the model does not develop bias through both pre-emptive and reflective measures. First, to try to avoid bias creeping in the model IRIS ensures that [REDACTED]

Second, fairness analysis is used to check whether the resulting model may still be biased [REDACTED]



29. Explain how you will notify individuals about the profiling.

Any personal data held in the [redacted] will be processed for the sole purpose of preventing fraud, error, and Debt. Disclosing information on specific Fraud and Error initiatives, by default, reveals how we are preventing and detecting fraud/error within our benefit system. We would run the risk of providing information that would help fraudsters and those intent on committing crime to know what data, controls, and systems DWP has in place to prevent and detect fraud.

Advances Model

The Advances model is trained on personal data of previous UC claims, [redacted]



The use of profiling to predict fraud and error by DWP is covered under the **Personal Information Charter**. This is to ensure individuals are informed that profiling will be undertaken by the DWP for fraud and error purposes.

Law enforcement

Only complete this section if the purpose of your initiative is the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

30. Explain how you will track access and changes to the personal data.

As a minimum you must track the following actions:

- collection
- alteration
- consultation
- disclosure (including transfers)
- combination (with other data)
- erasure

31e Explain how you will distinguish between the personal data of different categories of individuals and why you are processing the data for criminal law enforcement purposes for each category.

For example, categories of data subjects could be:

- individuals suspected of committing a criminal offence
- individuals convicted of a criminal offence
- individuals who are or may be victims of a criminal offence
- witnesses or other persons with information about offences

N/A

Section 2: Risk assessment

You must identify and assess any data protection risks in your initiative. The DPO team will help you. You should include risks to the rights and freedoms of individuals, and also corporate risks to DWP. The DPO team will suggest mitigations to reduce or eliminate each risk.

Use [standard DWP risk methodology](#) to assess risks: 1 = very low, 5 = very high.




- **Inherent risk score** – The level of risk before any action is taken to manage it and before mitigations have been put in place.
- **Residual risk score** – The level of risk at the time the DPIA is assessed. Some risks may already have been fully or partially mitigated and some may not have been mitigated at all.
- **Target risk score** - The projected risk score once all mitigations have been successfully implemented.

If there are high risks that cannot be mitigated, or that remain high even after mitigations are in place, it is a legal requirement that DWP must consult the ICO before the processing can take place. The DPO team will tell you if this is necessary.

You must continue to monitor these risks throughout the lifecycle of your initiative. You should add data protection risks to your initiative's risk register if you have one.

Risk description <small>Describe the source of the risk and the nature of the potential impact on individuals</small>	Inherent risk score <small>Impact x Likelihood</small>	Current mitigations	Residual risk score <small>Impact x Likelihood</small>	Planned or suggested mitigations	Target risk score <small>Impact x Likelihood</small>
<p>There is a risk that the historic personal data used to train the model may contain socially constructed biases, inaccuracies and mistakes that can affect the accuracy of the outcomes. This could lead to negative impacts for the individual and DWP could be in breach of the accuracy principle</p>	<p>[REDACTED]</p>	<p>Significant levels of testing were completed that allowed improvements to the model to minimise biases where possible within the model. IRIS [REDACTED] also deploy techniques to ensure that the model does not develop bias through both pre-emptive and</p>	<p>[REDACTED]</p>		

<p>There is a risk that the use of profiling to identify and prevent potential fraud could produce outcomes which could be seen to be unfair. This could lead to negative impact for the individual and DWP could be in breach of the fairness principle.</p>	<p>[REDACTED]</p>	<p>reflective measures. Fairness measures have been implemented which include significant training and testing of the model, [REDACTED]</p>	<p>[REDACTED]</p>		
<p>There is a risk that the historical personal data used to train the data will not be identified and included in a right of access request if it is held beyond the standard department retention policy. This could lead to an individual being unable to exercise their right of access.</p>	<p>[REDACTED]</p>	<p>Retention period of 14 months will be applied to the training data this is in line with DWP's retention policy. This will allow it to be identified and included if a customer makes a right of access request.</p>	<p>[REDACTED]</p>		
<p>There is a risk that the personal data used to train the model will be held longer than the standard</p>	<p>[REDACTED]</p>	<p>Retention period of 14 months will be applied to the training data this is in line with DWP's</p>	<p>[REDACTED]</p>		

<p>department retention policy as it may be needed to defend future legal claims. This could lead to personal data being held longer than necessary and DWP being in breach of the storage limitation principle.</p>		<p>retention policy.</p>			
<p>There is a risk that DWP are not meeting their transparency obligations as individuals may not be aware that they have been subject to profiling or that/how their data has been processed using artificial intelligence. This could lead to breach to an individual's right to be informed and the transparency principle.</p>		<p>DWP's personal information charter covers the use of profiling individuals are made aware of the personal information charter when making a claim for universal credit.</p>		<p>Update the personal information charter to include the department's use of artificial intelligence. Detailed information on Artificial Intelligence will not be divulged due to the sensitivities of the model.</p>	

Section 3: Sign off

Only complete this section when asked to do so by the DPO team.

Summary of DPO advice:
<p>This initiative is focused on the use of Common Risk Engine [REDACTED] which will enable transactional risking within the Universal Credit [REDACTED] to prevent fraud and error. [REDACTED]</p> <p>[REDACTED] This DPIA solely focuses on [REDACTED] attributed when a claimant makes a claim for an advance under Universal Credit.</p> <p>The use of [REDACTED] to determine potential fraudulent advance constitutes profiling. As individuals applying for an advance will be subjected to profiling there are risks associated with the fairness and accuracy of the proposed processing activity. As the outcome could potentially delay or lead to a refusal of an advance it is important that the model is producing accurate outputs. Therefore, the personal data and historical data used to train the model should be carefully selected and monitored to ensure that it is free from bias, inaccuracies, errors or mistakes that could impact the accuracy of [REDACTED] the outcome. The model should be continuously tested, and outputs analysed to ensure that it is operating as intended and that bias/discrimination has not developed over time.</p> <p>[REDACTED]</p>

[REDACTED] is a counter fraud initiative that uses Artificial Intelligence (AI) and Profiling so the project needs to consider how the transparency obligations will be balanced with the need to protect the counter fraud initiative. Profiling is currently covered under the DWP's Personal Information Charter. It will also be updated to reflect DWP's use of AI to ensure that transparency obligations are met and that individuals are informed. Detailed privacy notices are not being considered at this time in order to protect counter fraud initiatives. [REDACTED]

If the claim data used to train the model needs to be retained longer than the standard retention period UC claims, for example, to address potential legal challenge you this assessment will need to be revisited. This is because this can impact some of the individual rights. If you decide to keep data longer then you will need to consider how individual rights request will be facilitated.

Changes to your initiative

If there are any changes to your initiative that result in a change to the nature, scope, context or purposes of the personal data processing you may need to update this assessment. Get in touch with us if you're not sure.

Corporate records

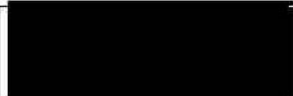
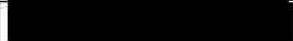
It is your responsibility to retain this screening assessment as part of your initiative's documentation, for example in your [registered file](#).

DPO advice provided by:	[REDACTED]
Date:	[REDACTED]

To be completed by, or on behalf of, the senior person (usually SCS) responsible for this initiative:

I understand and accept the advice provided by the DPO Team.	YES
I understand and accept the risks as described in the risk assessment.	YES
I agree to put the mitigations in place as described in the risk assessment.	YES
I agree to keep this DPIA under review and will seek further advice if there are changes to the nature, scope, context or purposes of the processing.	YES
If you answered NO to any of these statements, you must explain why:	

If you sign on behalf of the senior person responsible for this initiative, you must have their official authority to do so. The senior person (usually SCS) is accountable for any data protection risks associated with this initiative. A copy of this DPIA will be sent to the senior person named on page 2 of this form.

Signed by, or on behalf of, the senior person responsible for this initiative:	
Date:	

It is your responsibility to retain this DPIA as part of your initiative's documentation, for example in your [registered file](#).