



Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project or plan. It will enable you to consider privacy risks and the rights of freedom of individuals from the beginning of the project. It is a key part of your accountability obligations under the UK GDPR and is also a legal requirement under the legislation for certain types of personal data processing.

[For more details about the DPIA process, click here.](#)

[C&IR Information Security and Privacy - Policies, Procedures, Standards](#)

**You should complete all worksheets which appear in this file. Worksheets will be added depending on some of your answers.
Your C&IR consultant will fill in sections marked for them and the Comments boxes.**



Project Name Decision Intelligence PoC

What is this DPIA related to? Other

Business Process owner

Project Lead/ Representative

C&IR Advisor

Date of Engagement Mar-26

What part of the business is undertaking this project? Data, Technology & Innovation

>>>

Intelligence & Digital

Mark if this DPIA is related to a trial or proof of concept, not production use of personal data ☒

Purpose and Aim

Summarise the scope of the work and the purpose of the data processing.		
What are the key benefits or outcomes for the individuals whose data is being collected/used?	The DIP PoC does not provide direct, immediate benefits to individual data subjects. However, it is expected to deliver clear indirect and public interest benefits through improved regulatory outcomes. By enabling the FCA to better connect, search, and analyse information, the PoC supports earlier and more accurate identification of potential harm, improved prioritisation of regulatory activity, and more informed decision making. This contributes to more timely and targeted regulatory interventions, which benefit individuals by reducing the likelihood, scale, and duration of consumer harm, financial misconduct, and market abuse. Improved intelligence quality and decision support also help reduce the risk of inappropriate, inconsistent, or overly intrusive regulatory action, supporting fairer outcomes for individuals and firms. In the longer term, the PoC is intended to inform the development of more efficient and proportionate regulatory capabilities, supporting market integrity, consumer protection, and public trust. These benefits are delivered alongside strong safeguards to protect individuals’ rights, including data minimisation, restricted access, time limited processing, and secure deletion of data at the end of the PoC.	Comments Comments

What are the expected benefits for the FCA / PSR or related stakeholders?

The DIP PoC is expected to deliver benefits by strengthening the FCA's ability to carry out its statutory regulatory functions more effectively and proportionately.

This supports more timely, targeted, and consistent regulatory interventions, improving regulatory outcomes while reducing inefficiencies caused by fragmented systems and duplicated effort. Any harm found will be acted upon through the relevant internal processes

The PoC also provides evidence to inform future investment and design decisions, reducing the risk of deploying unsuitable or ineffective solutions at scale. By testing capabilities in a controlled, time limited manner, the FCA and PSR can assess whether proposed approaches improve effectiveness, efficiency, auditability, and governance before any wider rollout.

For related stakeholders (including operational teams and partner functions), the PoC supports improved access to relevant information, reduced manual effort, and clearer intelligence workflows, while maintaining strong safeguards around data protection, security, and accountability.

Comments

Are these individuals expecting the FCA / PSR to use their data for, (a) the agreed purpose, and (b) in the proposed way?

Yes, to the extent reasonably expected in the context of the FCA's statutory functions. Individuals whose data is processed within the DIP PoC have typically provided information to the FCA, or had information about them collected, in the context of the FCA's regulatory, supervisory, enforcement, and intelligence gathering activities.

Taken together, the PoC represents a fair, proportionate, and transparent extension of existing regulatory processing, rather than an unexpected or intrusive new use of personal data.

The FCA has taken steps to minimise potential intrusion or impact on individuals' rights by limiting dataset scope, [REDACTED]

Comments

Commentary on very limited use of employee data in "Detail" tab.

Nature of processing

Estimate the likely number of individuals' data that will be processed and how much data about each will be processed and over what time-period.

Mark if personal data will be used for **monitoring** of individuals purposes (such as CCTV/ surveillance, call or video recording, D&I or employee monitoring).

Mark if personal data will be processed for **tracking** individual’s online or offline geo-location or their behaviour/ habits.

Mark if the personal data will be used for systematic and extensive **profiling** with significant effects including denial of service based upon automated decision-making (used for profiling, evaluating or scoring).

Mark if there is a risk of **physical harm** to the data subjects.

Mark if personal data processing will include processing **criminal data**.

Mark if you have been advised that you should **work with the Information Disclosure Team** on subject access rights compliance.



several thousand people as one-off activity

☒

☒

☐

☐

☐

☐



☐



☐

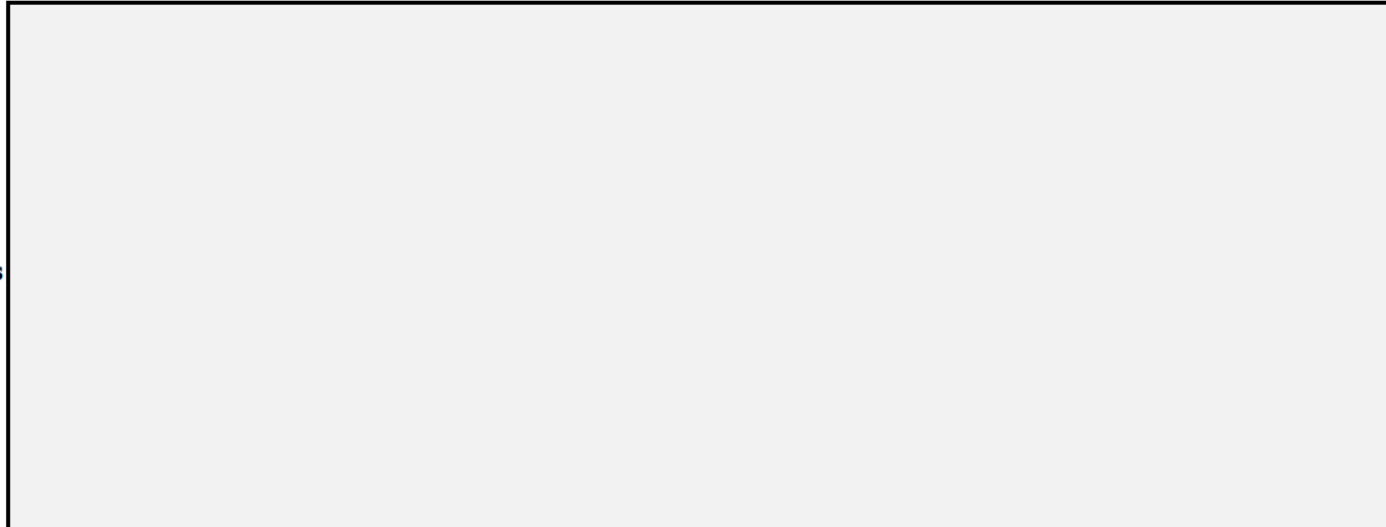
Comments

[Move on to the next tab >>>>](#)

[illegible]

Assess whether or not the data collected fits with the stated purpose of processing.

Comments



[illegible]

Describe how often the personal data will be collected.

The PoC is a one-off exercise to test the tool, using a one-off copy of data from FCA systems.

Comments

How will the data subject be aware that their personal data is being processed by the FCA/ PSR and other parties?

Data subjects will be aware of how their data is being processed by reference to the FCA's existing communications and privacy notice. These explain how data is used to support the FCA's regulatory and supervisory functions, as well as the use of third-party and IT service providers to support our operations.

Given the rise in prevalence of AI tools, a decision was taken to add explicit reference to how data may be used for the development and testing of AI and advanced technologies in October 2025.

For FCA staff, reasonable efforts are being made to remove employee data from the POC where possible, and it only being name and e-mail address and work phone being used if they are kept in the system. Employees are informed about the Palantir project and any use of personal data through PULSE articles.

[Public privacy notice](#)

[FCA Employee Privacy Notice](#)

[FCA internal PULSE article - "Fighting crime and our work with Palantir"](#)

[FCA internal PULSE article - "Update to the recent Pulse article on our work with Palantir"](#)

Comments

[Redacted]

[Redacted]

Comments

What is the retention period for the data being processed?

The data held in the PoC system will be used for the 12 week PoC period and then fully deleted.

How will this retention period be enforced?

The PoC environment is time limited by design. Data ingestion occurs as a one off exercise and no ongoing feeds are configured. At the end of the three month PoC period, all FCA provided data and any derived artefacts (including indexes, logs, and analytical outputs) are securely deleted from the supplier hosted environment.

Deletion is enforced through contractual obligations, technical controls within the hosting environment, and FCA oversight. Confirmation of deletion will be obtained from the supplier as part of PoC closure activities, ensuring that no personal data persists beyond the approved retention period. Also, the FCA will connect to the system and check the data has been deleted from the PoC system before the system is disabled.

Comments

[Move on to the next tab >>>>](#)



Data Protection Impact Assessment



Party involved in data processing	Controller/ Processor
FCA	Sole Data Controller

Third Party 1		Select 3rd party arrangement	New 3rd party
Palantir	Processor		
Add link to the contract or DSA			

Third Party 2		Select 3rd party arrangement	
	-		

Third Party 3		Select 3rd party arrangement	
	-		

This section to be completed by C&IR Consultant

Palantir	Has supplier due diligence been completed?	Yes
	Notes and comments on supplier and security posture	Reviewed security standards documents in Palantir Trust Portal. Details acceptable.



Data Protection Impact Assessment
Security of Personal Data Processing

Data Flows and Data Location

Include a data flow diagram, or link to a data flow diagram document.

Select if personal data will be held in SharePoint

☐

Systems in which personal data is stored

(other than SharePoint)

Describe how personal data will be transferred between systems and locations.

All data transfers and processing take place within the UK only.

Describe the security methods in place to ensure data transfer is secure.

Comments

Comments

Principle of Least Access

Described the user groups who will access the personal data.		Comments	
How are users given approval or access to the data?		Comments	
When and how are access rights reviewed to ensure only users with valid need have access?	Access rights are reviewed at the start of the PoC and monitored throughout . All access is removed at PoC completion.	Comments	

Now make sure you've completed the additional tabs >>>>

Notes on security controls that are specific to this project that help protect the personal data.	All LLMs used within the platform are hosted on UK based infrastructure. Specifically: - are hosted on a dedicated instance within a UK region. - are hosted via within a UK region. - Open source models (e.g.) are hosted directly within the Palantir platform environment itself. In all cases, the following guarantees apply: - Geo restricted to UK. No data leaves UK infrastructure at any point during model interaction. - Zero data retention. Neither prompts nor responses are logged or stored by the model provider. All interactions are ephemeral. - No training on customer data. FCA data is never used to train, fine tune, or improve any model. - No third party access. Model providers do not access the content of requests or responses. These are dedicated model instances provisioned for Palantir customers, not shared public API endpoints. FCA customer administrators control which models are enabled and available via the .
---	---



Data Protection Impact Assessment
Artificial Intelligence Assessment

Explain why AI is being used for this processing, instead of alternative, possibly safer, methods

AI is used in this processing because the PoC aims to evaluate whether advanced search and analytical techniques can meaningfully improve the FCA / PSR's ability to identify connections, patterns, and potential harms across large, complex, and fragmented datasets that cannot be effectively analysed using manual or rule based methods alone.

[Redacted]

Comments

[Redacted]

Describe the purpose of AI processing the personal data. What are the intended outcomes?

[Redacted]

Comments

[Redacted]

Describe which personal data is being processed by AI.

[Redacted]

Comments

[Redacted]

Are special category data being processed by the AI?  ☐

Mark if R&CO Data Front Door have completed their assessment ☐

AI Processing Activities

Select the processing activities that are being performed by AI.

- Profiling or categorising an individual or their data ☐
- Summarise content or create an analysis ☐
- Produce a yes/ no or pass/ fail result ☒
- ☐