Data Security & Privacy Lifecycle Expectations

# Data Security & Privacy Lifecycle Expectations

Below are a series of data security and privacy expectations of Ministry of Justice (MoJ) projects at various stages in their lifecycle.

These measures can help simplify and ease the burden of embedding data security and privacy at the heart of projects.

## Pre-Discovery and Discovery

Assess the data security and privacy implications of the project requirements thoroughly. Do this as part of the broader work addressing the project's strategic imperatives.

In particular:

* From the start of the project, and throughout its duration, think about how data security and privacy might affect the functionality and delivery of the project.
* Consult with technical architects to help inform and enhance the ways of delivering the work, whilst continuing to ensure compliance.
* Discuss any problems or ramifications that arise with legal or business experts. Identify areas where the required data security and privacy compliance might cause issues for functionality.

## Alpha

During this stage of the project lifecycle, internal and external (Cabinet Office / Government Digital Service) teams will perform service assessments. These will specifically check for aspects of GDPR/DPA18 compliance.

In particular:

* >That the majority of compliance considerations have been addressed at this stage.
* That the development team can say how their work ensures compliance.
* That the technical architecture choices can be tested against data security and privacy requirements. As an example, blockchain technologies might not be acceptable as they can prevent automated removal of information when it is no longer required.

## Beta (Private and Public)

These are assessments performed as the service transitions from Private to Public availability. The assessments are again performed by internal and GDS teams. Use live systems for the assessments.

In particular:

* All manually actionable data security and privacy requirements must be met.
* Manual testing is expected.
* Automatic deletion is not required yet, because the service is unlikely to have enough data at this stage. However, plans and mechanisms for automatic deletion should should be in place.
* Data should be backed up exactly as expected for a live service.

## Live

These are the final (Live) service assessments. They are again performed by internal and GDS teams.

In particular:

* Data sharing aspects might not yet be fully defined. Other consuming or supplying systems might not have established dependencies on the information shared.
* Some aspects of reporting might still need manual action. The newness of the system makes business MI requirements a work-in-progress.

## Post-Live (Ongoing)

These are the tasks that enable the final aspects of security and privacy for your project.

In particular:

* The final automated tasks are ready. The project cannot close until these are done.
* Data security and privacy compliance checks move to an ongoing status. Reporting takes place as required to internal stakeholders or the ICO.
* Schedule and run regular data mapping exercises. These ensure full and current understanding of data flows to and from any organisations or systems that depend on the information.