Data Security & Privacy Triage Standards

# Data Security & Privacy Triage Standards

Below are a series of common area guides from Ministry of Justice (MoJ) Digital & Technology Triage Standards.

## Purposeful Capture of Data

Only collect or store data if it is relevant, and needed for a specific purpose or task.

Ensure that:

* Everyone on the team understands why specific data is collected and stored. They should be able to justify this, backed with legal reasoning, as required.
* Each product has a clear privacy notice, describing how any personal data is handled. The notice contains a clear description of what we will do with their information, why, and how. Write it in terminology the general public can understand.
* Using an individual's information is only for the specific purposes or processes for which it was captured. There should be no superfluous information stored.
* The privacy notice describes any use of information for management or reporting purposes. Anonymise any personal information used for these purposes. In other words, before use, remove any fields or data that could identify the individual.
* You justify any special categories of needed information. The [Information Commissioner's Office (ICO)](https://ico.org.uk) - the UK's independent regulatory office for data protection - has outlined [a list of special categories](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/#ib3).

## Amending/Deleting Data

EU GDPR & the UK Data Protection Act (2018) requires that individuals agree to the handling and processing of their personal information. Many systems will need processes, to change, prevent, or stop handling personal information. The process might be have to be manual. Quite apart from GDPR/DPA18, these capabilities are generally useful for all MoJ systems.

Ensure that:

* The system has a defined retention schedule. These are normally drawn up between the SRO and the legal team. They detail how long we can keep information in the system before we must delete it.
* The system can delete records automatically at the end of the retention period. It should also be possible to remove records manually if required.
* Decisions or processes made using an individual's information can be stopped upon request.
* Ensure that information can be amended or re-examined manually, if necessary.
* If deletion is not possible, the system must be able to strip all identifying information from the records. This should make it impossible to identify an individual. Anonymising data should make it fall outside of the GDPR remit. The privacy notice should also mention this.

## Security / Architecture Considerations

Much of the MoJ estate architecture is ready for GDPR/DPA18, or transformation is already in progress. Current projects must also incorporate data security and privacy mechanisms for GDPR/DPA18 compliance. Guidance from technical architects is essential to help projects. Ensure that:

* You know where data for the system is stored. Ask which countries and jurisdictions hold the data. Check that the storage complies with GDPR/DPA18 requirements.
* The procedures to follow in response to a data breach are clear. Developed them with the help of the live service and cyber security teams.
* There is 100% confidence that data is backed up and protected against loss or other threat scenarios. Test and challenge this confidence frequently. Always test within the timescales defined in the retention schedule.
* The IA register lists the system. For potentially sensitive or risky data sets, check that the risk register also lists the system.

## Sharing Information

Many systems depend on data from more than one source. For example, data might come from cross-estate and cross-government levels. This makes accountability for the data vital: who owns it, and who is responsible for it.

Acceptable information sharing involves two distinct perspectives:

1. Sharing with other systems. There must be public transparency and understanding about using the information. Similarly for any dependencies on the information. To provide this detail, create data maps with the help of the system technical architects. Make sure that the maps include correct links between the data controller who originated the information and any other processors of the data.
2. Sharing with other organisations. There must always be an auditable record of the agreement between the organisations. This could be part of a contract, a data sharing agreement, or other general memorandum of understanding. Review the record at regular intervals so that it still meets the user or business needs, and continues to be relevant.

## Subject Access Requests

At any time, a person about whom we hold personal data can request a copy of all the information we hold about them. This is not a new requirement, and was part of original data protection legislation.

However, the £10 fee charged before is now waived. This makes it likely that there will be more Subject Access Requests in the future. Design your product to make it as simple as possible to perform Subject Access Requests quickly and easily. Authorised individuals from across all data storage locations should be able to respond.

## Law Enforcement Directive (L.E.D.)

Some systems hold information about criminals or criminal offences. This is sensitive data. An additional regulation applies to them: the Law Enforcement Directive.

Affected systems must record whenever an individual record is viewed or amended. Keep this log for audit purposes.

## Project Lifecycle Data Security and Privacy Expectations

When developing a system, there are some measures you can take that will simplify and ensure timely GDPR compliance.

### 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 (GDS) teams will perform service assessments. These will specifically check for aspects of GDPR 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.