Data Security and Privacy

# Data Security and Privacy

We believe that our technology must keep data safe and protect user privacy.

Our digital projects contain important information. Serious data breaches might result if we fail to:

* protect information
* handle it correctly at all times
* dispose of it safely when it is no longer required

Breaches might cause:

* harm to individuals
* financial loss to the Ministry of Justice (MoJ)
* a loss of confidence in us as an organisation

For personal data, the EU General Data Protection Regulation (GDPR) and UK Data Protection Act (2018) apply. These make the consequences of data breaches very clear.

To follow the data regulation/legislation, we **must** ensure that:

* we protect data to the best of our organisation's capabilities
* we collect data only for described, lawful purposes
* we use data only for the described, lawful purposes

## Why are security and privacy important?

Breaches can have an adverse effect the relationship between citizen and government.

Not only do we have a duty to protect citizens data, but the penalties for violations are also severe. Under the GDPR, serious infringements can result in fines of up to €20M.

We must apply appropriate security and privacy protection to all the information we hold and process, at all times.

We should treat all data as sensitive unless proven otherwise.

All our work must follow this ethos.

## When this applies

This principle applies to **all** MoJ technology projects and business actitivies.

While GDPR applies only to personal information, all MoJ projects and tasks must have excellent data security and privacy characteristics. If they handle personal data, they must do so correctly. Projects must follow MoJ guidelines unless exceptional and approved circumstances apply.

You can design your product to handle personal information correctly. There are a small number of extra steps you will have to take. Remember that personal data includes anything which might identify an individual. Even online identifiers, such as cookies, are personal data.

The [Information Commissioner's Office (ICO)](https://ico.org.uk) - the UK's independent regulatory office for data protection - has published [guidance on how to determine what is personal data](https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf).

A Data Protection Impact Assessment (DPIA, formerly commonly known as a Privacy Impact Assessment or PIA) is required for all projects. There are some [exceptions described by the ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/).

## Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [itpolicycontent@digital.justice.gov.uk](mailto:itpolicycontent@digital.justice.gov.uk).