Data sovereignty

# Data sovereignty

The Ministry of Justice (MoJ) Senior Security Adviser, Chief Information Security Officer (CISO), Chief Technical Officer (CTO) and Data Protection Officer (DPO) have issued this guidance for MoJ business units and third-party partners across the MoJ supported by Digital & Technology and/or within scope of the MoJ Data Protection Officer (DPO) to explain the MoJ's position on 'data sovereignty' (where the processing of data, including personal data, may take place).

## Summary

At OFFICIAL level, subject to adequate, proportionate and standard information security controls, the Department is content to process, and allow third-party partners to process, data (including personal data) outside the UK.

This statement includes the SENSITIVE (marked as OFFICIAL-SENSITIVE) handling caveat advising that additional care may be required; it is not a separate classification and any data / information is subject to the same rules as OFFICIAL.

The MoJ does not by default or routine require 'UK only hosting' or 'UK only services' for data privacy, data protection or information security reasons.

## Data sovereignty questions

* Where is the data located (i.e. servers and storage), including any off-site backup locations?

Even if located in the UK can it be viewed, modified, copied or deleted remotely from another country?

* Who is managing the service (n.b. administrators may be based anywhere in the world)?

For example, Microsoft Azure's data centre is in the UK but the system administrators can be located in Brazil, New Zealand, US and etc.

* Where are all of these entities legally instantiated and located?

For example, Amazon Web Services has UK data centres but is nevertheless is a US company with global support staff.

The 'where' data is processed is the combination of the answers to the questions above and is much more than just where the servers and hard drives are physically located (data hosting).

As part of routine due diligence, including fulfilling legal obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act (2018), where data is processed in other legal jurisdictions the MoJ is to ensure that adequate safeguards, including where relevant Data Protection Impact Assessments (DPIAs), are in place to ensure data is secure and that the rights and freedoms of any Data Subjects are maintained.

## UK and the European Union

The departure of the UK from the European Union will not lead to a change in the MoJ's position.

The MoJ has no plans to inshore data (i.e. limiting and / or returning data to the UK) for privacy or security reasons, nor is the MoJ asking its partners (for example, commercial suppliers) to do so.

## Where to get help

* In the first instance, contact the MoJ Cybersecurity team - [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).
* The MoJ's Data Protection Officer - [privacy@justice.gov.uk](mailto:privacy@justice.gov.uk).