

Date: 1st July 2025
Our ref: FOI/25/014684/A

FREEDOM OF INFORMATION REQUEST REFERENCE NO: FOI/25/014684/A

I write in connection with your request for information dated 29/04/2025, received by Greater Manchester Police (GMP) for the following information:

I am writing to request information under the Freedom of Information Act 2000 regarding your force's cloud data storage practices and data sovereignty policies, particularly in relation to sensitive and regulated data. If data is stored at an individual police station or unit level rather than force-wide, please provide it in that format.

Please provide the following information:

Q1 - Does your force currently store or process any sensitive or confidential data, including personal data, using cloud-based services?

Q2 - Can you confirm whether all patient and sensitive data is stored exclusively within UK borders?

Q3 - Please provide the names of the cloud service providers currently used by your force and the geographical locations (city/country) of the data centres where this information is stored.

Q4 - Do your force's contracts with cloud service providers include specific clauses requiring that data is stored exclusively within the UK?

If such clauses exist, could you provide a redacted copy or a summary of the relevant contractual terms?

Q5 - Does your force maintain a formal data sovereignty policy regarding sensitive or personal data?

If yes, please provide a copy of this policy or its key principles.

Q6 - Has your force conducted any formal risk assessments regarding data sovereignty or cross-jurisdictional data storage within the past three years?

If such assessments exist, please provide a summary of their findings and recommendations and when they took place.

I would appreciate it if the information could be provided in a digital format, such as an Excel spreadsheet or CSV file (if possible), for ease of analysis.

If any part of this request can be answered sooner than others, please send that information first, followed by any subsequent data. If it is not possible to provide any of this information due to exceeding the cost limit outlined in Section 12 of the Freedom of Information Act, please advise what information can be provided within the limit.

Should you need any clarification or have any questions regarding this request, please do not hesitate to contact me.

CLARIFICATION

To clarify, by "patient data," I intended to refer to "policing data," which includes sensitive law enforcement information such as criminal records, investigation data, personal identifiable information (PII), victim details, and other confidential data processed or stored by your force.

Result of Searches

Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate the requested information and I can confirm the information requested is held by GMP. However, I am not obliged to provide all the information requested as exemptions apply.

Section 17 of the Freedom of Information Act 2000 requires Greater Manchester Police, when refusing to provide such information (because the information is exempt) to provide you, the applicant, with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemptions apply

Part of question 3 has been exempt from disclosure by virtue of the following exemptions:

Section 24(1) – National Security

Section 31(1)(a)(b) – Law Enforcement

Section 31 and 24 is a qualified and prejudice based exemption and as such, subject to a harm and public interest test.

Evidence of harm:

Whilst not in any way questioning the motives of the applicant, it must be taken into account when considering potential harm that a disclosure under the Freedom of Information Act 2000 is made to the world at large, rather than a private correspondence. Releasing details about the geographical locations of data centres could pose a threat from hostile actors, who could use this knowledge to their advantage in an attempt to infiltrate one of our suppliers or exploit vulnerabilities in our products and use them to gain access to the forces' data which will include sensitive personal data as well as policing and investigative information.

The police service is charged with enforcing the law and protecting the public, and a successful attack, resulting in a significant data breach, could severely reduce its ability to carry out its core role of law enforcement and put individuals at risk of harm.

Public Interest Test

S24 – National Security - Factors favouring disclosure:

Disclosure would lead to a better informed public and the public are entitled to know how public funds are spent. The information simply relates to national security and disclosure would not actually harm it.

S24 – National Security - Factors favouring non-disclosure:

Operational systems and security measures are put in place to protect the community we serve. Disclosure of any such information that could place sensitive policing and investigative data which may or may not be linked to terrorism at risk, would highlight to terrorists and individuals' intent on carrying out criminal activity, vulnerabilities within the force.

Taking into account the current security climate within the United Kingdom, no information which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity.

Any incident that results from such a disclosure would, by default, affect National Security.

S31 – Law Enforcement - Factors favouring Disclosure

Confirming the geographical locations of data centres would be of interest to the public, namely reassuring them that data held by police is safely and securely stored.

S31 – Law Enforcement - Factors favouring Non-Disclosure

Measures are put in place to protect the community we serve. To provide details regarding data centres would allow individuals intent on disrupting law enforcement to target specific companies using the information obtained to maximise the impact.

Taking into account the current security climate within the United Kingdom, no information which may aid criminality should be disclosed. It is clear that it would have an impact on a Force's ability to carry out the core duty of enforcing the law and serving the community.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

Balance Test

For a public interest test, factors that favour disclosure need to be measured against factors against disclosure. It is important to note though that 'public interest' in this context is not what interests the public, or a particular individual, but what will be the greater good, if released to the community as a whole.

It is important that police forces are open and transparent, and in this case, this will help to further public knowledge in the software and services utilised. However, this needs to be balanced against the potential impact release could have on our ability to effectively carry out the law enforcement role.

The police service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. Providing information that would allow criminals to disrupt systems and access sensitive data would weaken our ability to carry out these roles; this cannot be in the public interest.

Therefore, it is my opinion that the factors for disclosure are outweighed by the factors against.

Response to remaining questions

Question 1 – Yes

Question 2 – Yes

Question 3 – Microsoft Azure UK

Question 4 – Yes. Please see the below clause.

- (a) where the Personal Data is subject to EU GDPR, not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the transfer is in accordance with Article 45 of the EU GDPR; or
 - (ii) the Processor has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the Controller which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the Controller;
 - (iii) the Data Subject has enforceable rights and effective legal remedies;
 - (iv) the Processor complies with its obligations under the EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations);

Question 5 – GMP does not have a specific sovereignty policy. Organisational procedure surrounding the governance of personal data is covered by GMP Data Protection Policy.

Question 6 – No formal risk assessments were conducted. However, there are a number of existing GMP policies governing the Force's procedures on the storage and processing of personal data.