



**Information Governance Team**

Postal Address:  
Coventry City Council  
PO Box 7097  
Coventry  
CV6 9SL

[www.coventry.gov.uk](http://www.coventry.gov.uk)

E mail: [infogov@coventry.gov.uk](mailto:infogov@coventry.gov.uk)

Phone: 024 7697 5408

09 March 2026

Dear Sir/Madam

**Freedom of Information Act 2000 (FOIA)  
Request ID: FOI796467713**

Thank you for your request for information relating to Palantir Contract (follow up to request FOI756976895).

You have requested the following information:

**1. If the contract has or is to be renewed with Palantir by Coventry City Council?**

Yes, it has been renewed for a further year.

**2. If it is to be renewed, how will the data on the AWS be managed considering it is not 100% sovereign and is subject to the USA's CLOUD Act?**

It will be managed in accordance with the terms of the contract which outlines the data transfer and hosting provisions. The data remains under the control of Coventry City Council as a Data Controller. The US Clarifying Lawful Overseas Use of Data (CLOUD) Act came into force on 23rd March 2018. Its purpose is to help with investigations relating to serious crime (including terrorism, violent crime, the sexual exploitation of children and cybercrime) by allowing the US government to demand data from electronic communications service providers and remote computing service providers. It extends to cloud storage providers. Please be advised that there are defined legal processes that must be followed before the US government can make a demand for data under the US CLOUD Act. These rules are set out in the US Stored Communications Act (SCA) which require the US government to:

- Obtain a warrant to seek access to electronic communications that has been in electronic storage for up to 180 days. The warrant can only be obtained if the US government demonstrates 'probable

cause' that the communications will establish evidence of a crime. A warrant 'may only permit searches of particular places for particular things' and is therefore not an instrument which gives the US government carte blanche to request bulk data indiscriminately.

- Use a subpoena or a court order if it seeks access to an electronic communication that has been stored for more than 180 days. Again, this must be a focused request which demonstrates there are reasonable grounds to believe the contents are relevant to an ongoing criminal investigation.
- Access to personal information requires a warrant, subpoena, or a court order. Again, this must be a specified request and cannot be used to request the release of bulk data records.

Upon receipt of a demand for data, a Cloud Services Provider (CSP) can apply to have quash or modify the warrant, subpoena or court order if the target of the demand is not a US person and that person does not reside in the US or if disclosure would create a material risk of violating an overseas nation's law.

Please be further advised that the UK has an existing data sharing agreement in place with the US, the 'Access to Electronic Data for the Purpose of Countering Serious Crime', which came into force on 3rd October 2022. This agreement provides a government-to-government mechanism to resolve conflicts over data access requests. Therefore, it is likely that a request to share data would be made under this provision, rather than the CLOUD Act. Again, this would only be in specified circumstances for defined purposes, as it is not a carte blanche mandate for the US government to seize large data sets from CSPs.

In terms of the specific contract referred to in your request, please be advised that the customer data remains within our control and it is legally and technically impossible for the service provider to comply with a request for customer data without our assistance. The council has therefore determined that there are sufficient safeguards in place which protects the data within its control. Any such request to share data by the council would be considered on a case-by-case basis, and data will only be shared where it is lawful and appropriate to do so.

### **3. If it is to be renewed, then how will the council manage legal enquiries about their data from the 11,000 plus families who may question why their data is open to USA regulation and conflicts with UK data protection and processing laws?**

We currently publish a suite of Privacy Notices on our website. We are currently reviewing these to make sure they are ultra transparent about our processing to allow those for whom we process their personal data to be well informed about their information rights.

The supply of information in response to a FOI/EIR request does not confer an automatic right to re use the information. You can use any information supplied for the purposes of private study and non-commercial research without requiring further permission. Similarly, information supplied can also be re used for the purposes of news reporting. An exception to this is photographs. Please contact us if you wish to use the information for any other purpose.

For information, we publish a variety of information such as: [FOI/EIR Disclosure Log](#), [Publication Scheme](#), [Facts about Coventry](#) and [Open Data](#) that you may find of useful if you are looking for information in the future.

If you are unhappy with the handling of your request, you can ask us to review our response. Requests for reviews should be submitted within 40 days of the date of receipt of our response to

your original request – email: [infogov@coventry.gov.uk](mailto:infogov@coventry.gov.uk)

If you are unhappy with the outcome of our review, you can write to the Information Commissioner, who can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or email [icocasework@ico.org.uk](mailto:icocasework@ico.org.uk).

Please remember to quote the reference number above in your response.

Yours faithfully

**Information Governance**