Department for Exiting the European Union

Freedom of Information Team
Correspondence Unit
9 Downing Street
SW1A 2AG

foi@dexeu.gov.uk
www.gov.uk

Rachel Mawhood
Via: request-449739-7f799e17@whatdotheyknow.com

Our ref: DEX000896

22 June 2018

Dear Rachel Mawhood,

FREEDOM OF INFORMATION REQUEST REF: DEX000896 - INTERNAL REVIEW

Thank you for your email of 9 February 2018 requesting an internal review of your request made under the Freedom of Information Act 2000 ('the Act'). I have now completed the review. I sincerely apologise for the time taken to complete the review and provide you with a substantive response. The Department for Exiting the European Union, (DExEU), aims to complete all requests for an internal review within a maximum of 40 working days, however, this is not always possible.

The Request

On 30 November 2017 you asked for the following information:

> *At the moment, some (perhaps all) Government departments e-mail is handled by Symantec MessageLabs ("cloud" based service integrating messaging and web security services) on servers hosted in other EU countries (eg Germany and the Republic of Ireland). After Brexit, I understand, this arrangement is likely to be illegal under existing EU data privacy and protection laws.*
>
> *So far I have seen nothing in the media anywhere or in Government announcements about this being one of the 58 impacts of Brexit, so I should be grateful to be sent any information you may be able to disclose on*
>
> *(a) the UK Government's' planned "milestones" for seamlessly migrating government messaging, data transfer and web security services - including the new online criminal court - to data centre hosting within the UK after Brexit, so that email arrangements of Government departments - and their access to their own archived data and e-mail communications - do not vanish at 11.00pm on Friday 29 March 2019 (because no longer compliant with EU data privacy laws about not sending data out of the EU); and*

(b) how much this will cost the British taxpayer.

Our response of 18 January neither confirmed nor denied whether DExEU held any information within scope of your request citing the exclusion at section 31(3).

I have now reviewed our response, taking into account the points you made in your request for an internal review.

Consideration of Exemptions

Section 31(3) of the Act provides an exclusion from the duty to confirm or deny whether information is held where to do so would, or would be likely to, prejudice law enforcement. Our response of 18 January specified the subsections engaged in this case to be 31(1)(a)(b), and 31(2)(a).

Section 31 is a qualified exemption and the consideration of the public interest was explained. The public interest in providing assurance that effective arrangements are in place for our exit from the European Union was recognised, however, it was considered that confirmation or denial in this case would undermine system security. Therefore, the public interest was found to be in favour of maintaining the exclusion of the duty to confirm or deny whether any information was held.

I find that this was an overcautious approach. It is the accepted response to requests that seek information relating to specific software applications in use in central government departments. Section 31(3) is often cited (sometimes alongside s24(2) national security), in cases where software applications are, or could potentially be, under review. This is the correct approach to protect the information systems in use by not exposing any potential system vulnerabilities, which in turn would be of interest to those who would wish to exploit any perceived weakness, and attempt to hack information systems with the intent of accessing information illegally, or to cause criminal damage to a system. This consideration was the basis of our response.

However, in this case your request can be considered in the wider context of information security following the exit from the European Union, and I am able to provide some information regarding this.

As part of our withdrawal from the European Union the UK is seeking agreement on Title VII of the Withdrawal Agreement. It is important that the data and information, which has been exchanged before the end of the Implementation Period (and on the basis of the Withdrawal Agreement), is protected in accordance with high data protection standards. The Withdrawal Agreement will ensure these “stocks” of data, such as the Symantec MessageLabs as you mention, do not vanish on 29 March 2019.

The General Data Protection Regulation (GDPR) is directly applicable and automatically became part of UK law on 25 May and the Data Protection Act 2018 entered into force on the same day (25 May). Our data protection laws will therefore be fully aligned with the EU’s at our point of exit. The UK is seeking a new EU - UK relationship on data protection that will maintain the free unhindered flow of personal data between the UK and the EU. The recent publications at the links below set out what the UK position is with regards to the future partnership:

https://www.gov.uk/government/publications/framework-for-the-uk-eu-partnership-data-protection

https://www.gov.uk/government/publications/technical-note-on-data-protection

Conclusion

In conclusion, I find the engagement of section 31(3) to neither confirm nor deny whether any information is held in this case was an overcautious response, and I hope that the information provided here is helpful.

This response ends the complaints process provided by the Department. If you are not content with the outcome of your internal review, you may apply directly to the Information Commissioner. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely

J Millar
Information Rights Appeals
Freedom of Information Team