Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : b7918a33 | Jul 27, 2023, 04:06 PM

This week, *Hacking Healthcare*™ examines the long awaited and recently agreed upon EU-US Data Privacy Framework. We breakdown what this agreement is, why it is needed generally and for the healthcare sector specifically, and whether or not it is likely to withstand the legal challenges that it is expected to face.

Welcome back to *Hacking Healthcare*™

A New EU-US Data Privacy Framework

On July 10, 2023, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework (DPF) which entered into effect immediately. The European press release states that, "The decision concludes that the United States ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the EU to US companies under the new framework. On the basis of the new adequacy decision, personal data can flow safely from the EU to US companies participating in the framework, without having to put in place additional data protection safeguards."[i]

An adequacy decision means that the European Commission has decided that a third country or international organization ensures an adequate level of data protection compared to what such data would be subject to within the EU.[ii] Adequacy decisions were established under the General Data Protection Regulation (GDPR), and as a result, personal data can flow freely from the European Economic Area (EEA), which includes EU member states as well as Norway, Iceland, and Liechtenstein, to a third country without another layer of conditions.[iii]

The adequacy decision regarding the DPF follows a multi-year effort and debate over US intelligence agencies' ability to access EU citizen data, in which the two prior agreements were annulled by the European Court of Justice. Key to the adequacy decision was the introduction of a means of redress for when EU personal data may have been collected improperly by US intelligence agencies. This process will be handled through the newly created Data Protection Review Court (DPRC). The framework also builds on the Executive Order, 'Enhancing Safeguards for United States Signals Intelligence Activities' which included necessity and proportionality controls for data gathering by US intelligence agencies, and addressed concerns raised by the EU Court of Justice.[iv]

So, what *exactly* does the EU-US Data Privacy Framework do?

- Due to the adequacy decision, personal data can flow freely and safely between participating US and EU companies.
- US intelligence agencies' access to data is now limited to what is 'necessary and proportionate' to protect national security; agencies will adopt procedures to guarantee oversight of the new privacy standards.
- It established a two-tier redress system to investigate and resolve complaints of Europeans on the access of data by US intelligence agencies, which includes the creation of the Data Protection Review Court (DPRC).[v]
- It sets obligations for companies processing data transferred from the EU, including the requirement to self-certify that they adhere to the standards through the US Department of Commerce.
- It establishes rigorous and layered oversight of signals intelligence activities and ensures compliance with limitations on surveillance activities.[vi]

While the DPF is already in effect, it will be subject to periodic reviews conducted by a team of representatives from the European Commission, European data protection authorities, and US authorities. The first review will begin within a year of the adequacy decision to ensure that all elements of the framework have been fully implemented and are functioning properly.

Action & Analysis
Includes with Health-ISAC Membership

Congress
Tuesday, July 25
No relevant hearings

Wednesday, July 26
No relevant meetings

Thursday, July 27
No relevant meetings

International Hearings/Meetings
No relevant meetings
EU

[i] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721
[ii] https://www.dataprotection.ie/index.php/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations
[iii] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752
[iv] https://www.state.gov/executive-order-14086-policy-and-procedures/

[v] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087
[vi] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087
[vii] https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft
[viii] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8249089/
[ix] https://www.sixfifty.com/blog/eu-us-data-privacy-framework/
[x] https://www.sixfifty.com/blog/eu-us-data-privacy-framework/
[xi] https://www.dataprivacyframework.gov/s/
[xii] https://www.goodwinlaw.com/en/insights/publications/2023/07/alerts-otherindustries-dpc-what-companies-need-to-know
[xiii] https://www.bakerdatacounsel.com/data-privacy/the-new-eu-u-s-data-privacy-framework-in-half-a-dozen-faqs/
[xiv] https://www.jdsupra.com/legalnews/european-commission-adopts-an-adequacy-2034081/
[xv] https://www.alstonprivacy.com/international-data-transfers-european-commission-gives-green-light-to-eu-u-s-data-privacy-framework/

Report Source(s)

Health-ISAC

Reference | References

goodwinlaw
jdsupra
Europa Analytics
state
bakerdatacounsel
nih
sixfifty
dataprivacyframework
Health-ISAC
csis
alstonprivacy
Data Protection
Europa Analytics
Europa Analytics

Tags

Hacking Healthcare, International Law, EU, Information Sharing, Data Transfer

---

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.
John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org