Cyber Security for Europe

Policy Recommendation

Set up a data protection by design and by default technology programme

Context and Findings

Digital services and cloud markets are global and highly competitive, encouraging the transfer of European personal and business data both within and beyond Europe.

Not all non-EU territories provide an adequate level of cybersecurity or data protection to EU citizens' data, as has been demonstrated with high-level court cases[2] [3].

With its data protection by design and by default principle, the GDPR **requires appropriate technical and operational measures to be implemented to counteract high risks** involved with the processing and sharing of sensitive data.

In their 2020 set of recommendations, the European Data Protection Board suggests that **cross-border data transfer use cases can be protected by privacy enhancing technologies (PETs)**[1].

The European Union has invested in privacy enhancing technologies in numerous framework programs, but there has been **no notable or significant adoption in Member States**.

The Problem

European personal and corporate data does not enjoy the same level of protection in all territories outside Europe. While adequacy agreements have been negotiated, they have not been found to be compliant with European law by the Court of Justice of the European Union. Well-known, high profile examples of non-compliance cases include Schrems I[2] and Schrems II[3] but there are many more. New agreements are regularly negotiated and re-negotiated, but they may also be challenged in court, leading to a cycle where it is very complicated to develop business and research collaborations between EU Member States and many non-EU countries.

The Scene

PETs have been developed to reduce the need to process identifiable data in systems. While we are used associating privacy with personal data, the PET technologies can also be used to process business or government secrets. There has been notable investment into privacy technologies in the world. The European Commission has invested considerably developing PETs in recent Horizon 2020 projects as well as in earlier programs[4].

In the United States, DARPA, IARPA[5], the National Science Foundation and the National Institute of Health have probably invested even more heavily, in secure computing technologies alone. In the last five years, venture capitalists have also invested significantly in companies developing individual technologies like secure multi-party computation. The United Kingdom and United States have recently launched a set of prize challenges to unleash the potential of PETs to combat global societal challenges[6]. Singapore has launched a PET Sandbox to develop and pilot use-cases and to support businesses with PET projects[7]. While European legislation is rapidly developing to improve data protection and the data economy, technology adoption by Member States is lagging behind due to a lack of skills and lighthouse projects that could inspire new systems that use PETs to follow the data protection by design and by default principle in the GDPR.

The Implications

Europe is building new data-driven services using technologies and infrastructure from all around the world. Cloud service providers from other territories are offering competitively priced infrastructure and services that are becoming an integral part of our digital transformation. Many European websites are parts of global user tracking and advertising infrastructure that transfers data to other territories. Apps in our mobile phones are storing our identities and secrets, while also using technologies that monitor and share data. Europeans are losing control over that data together with the related identities and business models.

Similarly, our ability to collaborate in global research is reduced, as personal data collaboration with non-European researchers is hindered by the lack of tools supporting privacy-preserving research. This is a most pressing concern in health sciences, where developments in not only genomics and personalised medicine but also pandemic response require collaboration at the widest level with the freedom to share high volumes of sensitive data with confidence.

Policy Recommendations

We have three policy recommendations to support the adoption and implementation of European regulations and policies surrounding the data economy, the Digital Single Market and international trade agreements.

1) Support projects working towards exploring the role of PETs in reducing risk and advancing European data protection policy to promote the use of advanced PETs

There is a great need to push the boundaries of knowledge on what can be achieved with technologically enforced data protection. We need risk analysis methodologies that help us understand the risks and benefits of using different PETs. If we can categorize PETs by the level of re-identification avoidance provided (feasibility of re-identification), we can have a better estimate on what is the current state of the art and which technologies and which settings can be considered strong enough to protect sensitive and special categories of personal data.

Future Horizon Europe and Digital Europe calls working on data and security technologies of data should be encouraged to provide a re-identification risk analysis based on re-usable methodology. Different risk analysis methods work for different technologies, so multiple methodologies will need to emerge and reach a higher level of maturity. Re-use and extension of these methodologies should be encouraged to reach a higher maturity of re-identification risk analysis that leads to an increased uptake of PETs.

2) Initiate a PET lighthouse project programme

PETs have been used in a few European-scale systems, e.g. many of the exposure notification apps deployed to inhibit the spread of COVID-19. However, there are many areas where no successful blueprints for deploying PETs in Europe have been established, even though there is a great need.

We need a program that encourages projects that:

a) provide reusable technical and legal blueprints for a certain area or use case,
b) deploy PETs in production for public sector and public-private collaborations and
c) achieve a high technical readiness level (TRL 7-8).

The pilots should be aligned with the European Data Spaces initiative and other relevant programs. We believe that there is an opportunity to reuse the same collaboration that Europe has used for cybersecurity and blockchain innovations – a PET observatory, PET competence co-located with cybersecurity competence centres etc.

3) Launch selected PET lighthouse projects with the United States of America

As there are only a few funding and collaboration instruments that exist for joint EU-US research activities, developing technical controls to support secure data-related work with US research partners or to securely use US cloud infrastructures could have a high impact on enabling formal collaboration initiatives. Thus, we recommend having three separate EU-US project calls in Horizon Europe in collaboration with partners like the US National Science Foundation and the National Institute of Health to design and launch privacy technology pilots between European and US data owners, technology providers and regulatory experts. The three project calls should be in the domains of healthcare, financial crime prevention and cyber defence. We note that the healthcare project call could support both the European Commission's Conquering Cancer[8] and the US White House Cancer Moonshot[9] missions. This initiative could also collaborate with the EU-US Technology and Trade Council (TTC).

References

1 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. European Data Protection Board. Adopted on 10 November 2020. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

2 Schrems I, 6 October 2015: https://curia.europa.eu/juris/liste.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-362%252F14&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%2

3 Schrems II, 16 July 2020: https://curia.europa.eu/juris/liste.jsf?num=C-311/18

4 For example, UaESMC, PRACTICE, SafeDEED, SODA, CyberSec, SafeCloud and many others.

5 Intelligence Advanced Research Projects Activity

6 US-UK Privacy Enhancing Technology challenge: https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/

7 Singapore PET Sandbox: https://www.imda.gov.sg/How-We-Can-Help/Data-Innovation/Privacy-Enhancing-Technologies-Sandbox

8 European Commission Cancer Mission: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding- programmes-and-open-calls/horizon-europe/eu-missions-horizon-europe/eu-mission-cancer_en

9 White House Cancer Moonshot: https://www.whitehouse.gov/

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Dan Bogdanov dan@cybernetica.ee

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.