"Data Free Flow with Trust"

ROUNDTABLE OF G7 DATA PROTECTION AND PRIVACY AUTHORITIES
07 – 08 SEPTEMBER 2021

- Communiqué -

We, the data protection and privacy authorities of the G7 member countries, met on 7 and 8 September 2021 under the chairpersonship of the UK Information Commissioner, Elizabeth Denham CBE, to discuss opportunities for closer collaboration.

The meeting took place in the context of the Roadmap for Cooperation on Data Free Flow with Trust, announced by G7 Digital and Technology Ministers on 28 April 2021, and was a timely discussion in the context of the growing global, data-driven economy and the changes being driven by the ongoing pandemic.

- - -

More data is being generated, collected and used than ever before, with the global volume of data predicted to double between 2018 and 2022 and then double again between 2022 and 2025. Technological developments are at the heart of this rapid growth, with advances in areas from artificial intelligence to the Internet of Things (IoT) enabling wealth of data-driven innovation.

To uphold information rights in this digital age, data protection and privacy authorities need to become ever more effective at anticipating, interpreting, and influencing such advances in how data is used. To realise this ambition in a context where data flows seamlessly across borders and digital businesses reach customers globally – and build trust and confidence, underpinned by high standards of data protection – requires deeper and swifter international regulatory cooperation.

As the data protection and privacy regulators of the world's most advanced digital economies, we recognise that we can play a leadership role in discussions on these issues and help influence the adoption of high standards for data protection globally. We can identify areas of mutual concern or opportunity and respond with agility to ongoing developments, driving collaborative regulatory approaches that seek to create consistency and legal certainty where possible.

In recognition of this challenge, we discussed a number of specific key issues to share our expertise and experience and explore possible closer cooperation between the G7 data protection and privacy authorities. Topics on our agenda, listed in the order that they were discussed, included:

- **Privacy and Competition Intersection – Cross-Regulatory Collaboration to Support a Robust Global Digital Economy**

- **Shaping the Future of Online Tracking**

- **Designing Artificial Intelligence in line with Data Protection**

- **Redesigning Remedies for the Digital Age**

- **Pandemic-Driven Tech Innovation: A Stress Test for Data Protection Rights**

- **Government Access and Data Flow at International Level: What Role for Regulatory Cooperation in Ensuring Real Trust?**

- **Development of a Framework for Cross-Border Transfer of Personal Data and Cooperation between G7 Data Protection Authorities**

A summary of each topic and key points from the conversations is included in the Annex to this communiqué.

Agreed outcomes

As a result of the above discussions, we have agreed to:

Privacy and Competition Intersection – Cross-Regulatory Collaboration to Support a Robust Global Digital Economy

- Strengthen collaboration between the G7 data protection and privacy authorities and their domestic competition counterparts on the regulation of digital markets.

- Share experience and intelligence among the G7 data protection and privacy authorities, with the ambition of fostering consensus, setting norms, and facilitating practical actions towards mutually serving the objectives protecting individuals' rights and maintaining competitive digital markets.

- Advocate for greater collaboration between data protection and privacy authorities and competition regulators at global privacy and competition forums and networks, including through closer dialogue between the Global Privacy Assembly (GPA) and the International Competition Network.

Shaping the Future of Online Tracking

- Initiate a strategic dialogue between the G7 data protection and privacy authorities and technology firms, standards bodies, designers, web developers, users and civil society to examine the role that technological developments can play in creating a more privacy-oriented internet, upholding and preserving the principle of an informed and meaningful prior consent online.

- Continue to collaborate among the G7 data protection and privacy authorities on wider efforts to improve standards of data protection by websites, including by sharing experience and good practice.

Designing Artificial Intelligence in line with Data Protection

- Advocate for the central role that data protection and privacy authorities should play in the future governance of artificial intelligence.

- Create a dialogue among G7 data protection and privacy authorities on the principles that should govern the responsible development of artificial intelligence.

- Exchange intelligence and expertise on novel applications of artificial intelligence and the privacy implications arising from these.

Redesigning Remedies for the Digital Age

- Share information and experience on what regulatory remedies work best in particular situations.

- Advocate for legislators to ensure that regulatory remedies keep pace with technological change and maintain sufficient parity across jurisdictions.

Pandemic-Driven Tech Innovation: A Stress Test for Data Protection Rights

- Proactively demonstrate our commitment and ability to move quickly when needed, while continuing to ensure the high standards of data and privacy protection of our citizens.

- Advocate for innovation that effectively meets the public need and protects citizens' privacy, keeping pace with the development of new technologies, products and business models and maintaining our relevance to these emerging issues.

- Ensure that the proliferation of new technology seeded by the pandemic is both harnessed for good and achieves individual privacy and data protection rights.

Government Access and Data Flow at International Level: What Role for Regulatory Cooperation in Ensuring Real Trust?[1]

- Engage with our respective governments in support of progressing initiatives at international level, including at the GPA, the Council of Europe, the G20 and in particular the OECD's work on government access to personal data held by the private sector which offers a key opportunity to provide agreed principles that can govern this important topic.

- Share relevant developments in legislation and practice among G7 data protection and privacy authorities and coordinate our domestic advocacy and policy efforts to promote ambitious principles applicable to government access to personal data.

[1] This section relates to matters outside the jurisdiction of the U.S. Federal Trade Commission

- Develop constructive and appropriate relationships with other relevant domestic oversight bodies in our respective countries to ensure a consistent approach to privacy and data protection in the context of government access.

Development of a Framework for Cross-Border Transfer of Personal Data and Cooperation between G7 Data Protection Authorities

- Promote a more open and frequent dialogue among G7 data protection and privacy authorities, built on shared networks, regular meetings and ongoing discussions across our jurisdictions.

- Exchange experiences and practices in the governance of emerging technologies and innovations, with the aim of fostering interoperable regulatory approaches among G7 data protection and privacy authorities.

- Identify opportunities for greater enforcement cooperation among G7 data protection and privacy authorities, starting by developing a shared understanding of the legal frameworks and enforcement practices across jurisdictions, including on the scope for their extraterritorial application.

Looking to the future

This roundtable event has highlighted the benefits of continuing a discussion in this format as we each grapple with the ever-increasing challenges of regulating within our own jurisdictions for a data economy which transcends borders. We have therefore agreed that the BfDI will host a further such roundtable when Germany assumes the G7 presidency next year.

In the interim, we will continue to engage at working level to support the agreed outcomes of this roundtable and to help build a close knitted network of experts at the various G7 authorities.

Through this new forum, the G7 Commissioners have established a flexible environment in which they can discuss issues of mutual interest and seek to forge a longer-term relationship, voice and influence with international organisations and other key international stakeholders to promote our shared values and objectives as the data protection and privacy regulators of the seven most advanced digital economies.

ANNEX – SUMMARY OF TOPICS DISCUSSED

Privacy and Competition Intersection – Cross-Regulatory Collaboration to Support a Robust Global Digital Economy

Digital markets are transforming our economy and our society, with companies that began as start-ups scaling rapidly to deliver global change. In many ways these changes are for the better, with benefits to consumers, innovation and economic growth – but they present serious challenges too.

There are clear incentives for the collection and exploitation of personal data that come at the cost of individual privacy and create serious competition concerns. Confronted with such a seismic shift in the landscape, competition regulators and data protection and privacy authorities must work together to promote a robust digital economy, engendering trust amongst global citizens and holistically advancing their rights and consumer interests.

Given the nascent stage of the study of this intersection, close collaboration is needed between authorities on matters including: developing a common lexicon and approach to factual environments; identifying and mitigating potential trade-offs between protecting privacy and promoting competition; assessing how market failures can negatively impact citizens' privacy or cause competition authorities to overlook privacy as a competitive factor; and working towards enforcement remedies that achieve positive outcomes both from a competition and privacy perspective.

Shaping the Future of Online Tracking

Cookies and similar technologies can be used to collect data for a range of different purposes. While some cookies are essential to make a website work properly, others collect data for purposes which are not technically required to provide the service, such as to support targeted advertising. The extent of such tracking technologies should be reduced and users should have the choice of not being tracked at all.

The current system of repeated, frequent cookie consent mechanisms (e.g. pop-ups, banners) at the point of data collection by websites leads to a situation where most people reflexively select "I agree" – despite holding legitimate concerns about how their data is used. Moreover, users report that they do not have time to engage with complex or misleading cookie consent mechanisms and – while wanting more control about how their data is processed – feel powerless to stop the gathering of their data. Issues such as 'cookie walls' (where if users do not 'agree' to be tracked they may be denied website access) and 'dark patterns' (where the architecture of privacy notices is designed to trick users into providing consent) further serve to teach users that they cannot control their data.

Meaningful consent is frequently not being obtained. Action is needed to ensure that web users are able to meaningfully control the processing of their personal data as they browse the internet, in tandem with promoting high standards of data protection by websites and acting to tackle harmful practices. Web browsers, software applications and device settings all have a role to play in enabling people to set and update their lasting privacy preferences and ensure that these are respected by websites.

Designing Artificial Intelligence in line with Data Protection

Artificial Intelligence (AI) promises to help us overcome some of the biggest challenges we face in our world today. It can, for example, enable physicians to make better diagnoses and pursue new therapeutic paths. In seizing these opportunities, it must be ensured that the human right to privacy, the right to informational self-determination and other fundamental rights are not violated by the use of AI.

Data protection and privacy authorities must play a leading role in the governance of AI, which is built on data. They should constructively influence the developments of AI systems and create a framework that safeguards human rights, democracy, the common good, and individual freedoms while creating room for innovation and progress. "Red lines" are needed for AI systems that are not compatible with our values and fundamental rights. To fulfil this task, data protection and privacy authorities need sufficient human and material resources.

The complexity of global supply chains means that common principles are needed for the governance of AI. Human dignity must be central to AI design; AI must be transparent, comprehensible and explainable; and the data protection principles of purpose limitation and data minimisation must apply to AI. Further work is needed to foster the development of interoperable approaches to regulation of AI across jurisdictions, in the interests of people and businesses.

Redesigning Remedies for the Digital Age

The rapid evolution of the digital economy means that data protection and privacy authorities need to continually reflect on whether their enforcement toolbox is fit for purpose and their responses do enough to stop firms from benefitting from their illegal actions and dissuade others from engaging on the wrong side of the law.

It is paramount that any regulatory responses that data protection and privacy authorities take keep individuals who are fallen victims of these businesses at the centre of their considerations. Goals of remedies should include redress for consumers and affected citizens, accountability for organisations, a level playing field for business and deterrence of future non-compliance.

Remedies must keep up with the pace of technological change and development of new business models. Given the global nature of the digital economy, it is important that the remedies available to data protection and privacy authorities maintain sufficient parity across jurisdictions.

Pandemic-Driven Tech Innovation: A Stress Test for Data Protection Rights

For the last 18 months, our lives have been dominated by the Covid-19 pandemic. The measures that governments have taken to fight the pandemic, coupled with the proliferation of data processing resulting from a rapid uptake of digital services, have put stress on many of the fundamental rights and freedoms that are cornerstone of modern democracies, including the right to respect for private life.

The application of data protection and privacy laws must be flexible and contextual when responding to emergency or unprecedented situations, such as the pandemic. However, it is

precisely in such emergency situations where extraordinary solutions are deployed that data protection and privacy authorities must ensure that they act as both protectors and enablers, ensuring that citizens' data rights are upheld whilst appropriate responses to the public health emergency can be deployed.

Developing consistent approaches to the issues arising will allow us to continue to vigorously act as custodians of the values that define our societies, including to safeguard the protection of personal data.

Government Access and Data Flow at International Level: What Role for Regulatory Cooperation in Ensuring Real Trust?[2]

Governments and intelligence services have legitimate needs to access personal data. However, individuals' privacy and other human rights must be respected, and government access to personal data should be subject to appropriate safeguards and oversight.

Different rules in different countries, and uncertainty over public authorities' practices, may also lead to barriers to enabling cross-border data flows with trust. Conversely, a common understanding of the basis on which public authorities can have access to data, and the safeguards that should be in place to protect individuals, can help build the trust that underpins cross-border flows of data and thus alleviate potential restrictions on data flows.

While common underlying principles on how such access should be regulated are being discussed in other international fora, cooperation between G7 data protection and privacy authorities on this issue is important to help formulate and advocate solutions. This is with the aim of ensuring consistent protections and remedies for individuals when their personal data is being transferred between countries and supporting the free flow of personal data by overcoming current challenges and barriers, with high legal standards that offer real protection for the privacy rights of citizens around the world.

Development of a Framework for Cross-Border Transfer of Personal Data and Cooperation between G7 Data Protection Authorities

The pace of innovation and technological change has given rise to a global digital economy with massive transfers of data, including personal data, across borders and political systems. This presents a challenge to data protection and privacy enforcement authorities. Cooperation between regulators in different countries is essential to avoid regulatory arbitrage and protection of rights at different speeds and levels.

Data protection and privacy authorities need to share expertise and best practices and cooperate on investigations of cross-jurisdictional relevance, in particular where innovative technologies and new products and services are emerging. Developing a framework for collaborative, consistent and responsive enforcement policies and practices will both provide greater certainty for those we

[2] This section relates to matters outside the jurisdiction of the U.S. Federal Trade Commission

regulate as well as enable potential collective regulatory actions for the benefit of global communities.

- - -

We also welcomed interventions from the OECD and World Economic Forum on what issues they believe would benefit from cooperation between the G7 data protection and privacy authorities. These interventions provided us with valuable perspectives from colleagues outside the data protection and privacy community. We exchanged views on multiple challenging questions regarding transborder data flows.

The OECD presented on the importance of good data governance and cooperation between countries to cross-border data flows, how this ultimately benefits citizens economically, and the work that the OECD is doing to support this.

The World Economic Forum presented on how the movement of data across borders is crucial to the modern global economy, how well-intentioned policies in this regard can, in their view, give rise to adverse unforeseen consequences, and the consequent role that the G7's data protection and privacy authorities could play in shaping the global economy.