44th Closed Session of the Global Privacy Assembly

October 2022

Draft Resolution on International Cooperation Capacity Building for Improving Cybersecurity Regulation and Understanding Cyber Incident Harms (v1.9 final)

This Resolution is submitted by:

SPONSORS:

- Information Commissioner's Office, United Kingdom

CO-SPONSORS:

- Office of the Australian Information Commissioner, Australia
- Office of the Privacy Commissioner, Canada / Commissariat à la protection de la vie privée du Canada
- Superintendence of Industry and Commerce (SIC) of Colombia
- Estonian Data Protection Inspectorate, Estonia
- European Data Protection Supervisor, European Union
- Commission Nationale de l'Informatique et des Libertés (CNIL), France
- Ghana Data Protection Commissioner (GDPC), Ghana
- Gibraltar Regulatory Authority (GRA), Gibraltar
- Office of the Privacy Commissioner for Personal Data, Hong Kong, China
- Israeli Privacy Protection Authority (PPA), Israel
- Jersey Office of the Information Commissioner (JOIC), Jersey
- National Privacy Commission, Philippines
- Personal Information Protection Commission, Republic of Korea
- Catalan Data Protection Agency, Catalonia, Spain
- Swiss Federal Data Protection and Information Commissioner (FDPIC), Switzerland

- Turkish Personal Data Protection Authority (KVKK), Türkiye
- Regulatory and Control Unit of Personal Data, Uruguay.

The 44th Global Privacy Assembly 2022:

HIGHLIGHTING THAT a global economy and society brings a range of benefits such as global trade; the global spread of technology and innovation; communication, collaboration and the sharing of knowledge and resources to address global issues; and cross-cultural exchange, and that these benefits can only be properly realised if personal data is adequately protected;

CONCERNED THAT the increasing digitalisation of the global economy and society brings, alongside its benefits, increasing and significant risks to individuals' personal data held by public and private organisations;

NOTING THAT risk may include accidental but also deliberate threats such as surveillance and data access attempts from sources such as state actors and non-state criminal entities in many jurisdictions, often operating across borders;

RECOGNISING THAT confidentiality, integrity and availability, the three key elements of information security are at risk as a result of these threats; if any of the three elements is compromised, then there can be serious consequences for data controllers, and significant harms for the individuals whose personal data is impacted;

HIGHLIGHTING THAT a principle common to privacy and data protection laws around the world is that personal data should be protected by appropriate security safeguards against such risks as loss or unauthorised access, destruction, use, modification, disclosure or non-availability;

RE-EMPHASISING the importance of preserving public trust in the networks and IT systems through which personal data are processed, and the important role that strong data protection and privacy safeguards play against cyber threats;

NOTING THAT cyber resilience of data processing systems is being severely tested and media and security analysts have reported an increase in cyber attacks worldwide which may include supply chain attacks, unauthorised access, ransomware, identity fraud or phishing;

CONCERNED THAT cybersecurity incidents are now reported to have significant economic consequences for society, noted to be the top threat to organisations' financial success[1] and the potential trade barriers this can risk causing; and that these consequences also notably impact smaller and less well-resourced organisations who process personal data;

ALSO CONCERNED THAT organisations are not always taking the timely steps required to update technical and organisational measures, such as pseudonymisation or encryption, within legacy systems to be effectively equipped against increasing cyberattacks, which generates risks that data protection and privacy authorities have a role to address, in collaboration with others, and that

[1] Cybersecurity is reported to be the number one threat CEOs are concerned about from global survey by PriceWaterHouse Coopers, January 2022 (25th Annual Global CEO Survey – PwC). CEOs are most worried about the potential for a cyberattack or macroeconomic shock to undermine the achievement of their company's financial goals.

those risks are amplified if organisations fail to report such attacks, data breaches and other incidents when they happen or when they are discovered;

FURTHERMORE CONCERNED THAT a single cyber attack may have serious consequences for many victims in different jurisdictions; and *EMPHASISING* the resulting importance of avoiding duplication of regulatory work, which in turn demonstrates the value of cooperation on common threats both between GPA member authorities, and with cybersecurity bodies where appropriate and permitted by local laws;

HIGHLIGHTING the forthcoming OECD Recommendations on the digital security of products and services, and on vulnerability treatment, based on existing work conducted by the OECD's Committee on Digital Economy Policy in 2021 together with external experts, which promote security by design and by default in products and services, the use of security researchers' expertise to identify, report and disclose digital security vulnerabilities, as well as compliance strategies aligned with data protection law requirements;

NOTING THAT public policies have begun to evolve at the national level in strengthening protections of national critical infrastructure, including protection of public and essential services and ensuring accurate incident and data breach reporting. In doing so, Governments have recognised the close relationship required between data protection law/regulation and network information systems and security legislation, to design effective incident prevention, response and enforcement solutions, particularly where critical national infrastructure protection is concerned;

RECOGNISING that data protection and privacy authorities in different jurisdictions have very different responsibilities, competencies and powers in relation to cybersecurity; yet *NOTING* cybersecurity's close link with many data protection and privacy laws' requirements relating to security, confidentiality, integrity and availability of personal data;

REAFFIRMING the GPA's mission which includes connecting and supporting efforts at domestic and regional level, and in other international forums, to enable authorities to better protect and promote privacy and data protection; and the importance of capacity building, cooperation, sharing information and knowledge in furthering the mission;

RECALLING THAT the GPA's first strategic priority is to advance privacy in an age of accelerated digitalisation, and the relevance of cybersecurity in furthering that priority; and *FURTHER RECALLING* that the GPA Strategic Plan 2021-23[2] requires the GPA to monitor opportunities for cooperation, noting new and emerging digital risks posed to individuals' privacy;

RECALLING THAT the GPA has already recognised[3] that convergence towards key principles and high standards for government access to personal data held by the private sector may contribute to legal certainty and the facilitation of data flows in the global digital economy and has emphasised the importance of cybersecurity in and across all systems;

HIGHLIGHTING the importance of cybersecurity to data protection and privacy, and concerned that significant harms to individuals and in particular those from vulnerable groups can be caused by cyber attacks; among them personal data being obtained, matched and sold for fraudulent purposes;

---

[2] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)
[3] 20211025-GPA-Resolution-Government-Access-Final-Adopted .pdf (globalprivacyassembly.org)

NOTING that some data protection and privacy authorities have already started mapping cybersecurity harms in relation to other harms and identifying societal and individual harms from cyber incidents; but that more needs to be done to compare across jurisdictions: the harms rather than the abuses identified, (for example, physical, psychological, cultural, political, economic and reputational harm at both individual and societal level); the models used to assess or categorise these harms; gap analysis; and what the regulatory consequences should be;

HIGHLIGHTING that consequential harms of cybersecurity incidents are diverse and would merit further analysis about how best to protect individuals from those harms;

NOTING THAT governments in many jurisdictions are collaborating to protect national security and critical national infrastructure;

HIGHLIGHTING THAT data protection and privacy regulators must also stand ready to collaborate, as appropriate, on international and domestic strategies to protect individuals' data in relation to cyber incidents; and also that the GPA is well placed to promote effective regulatory data sharing between GPA Members on cybersecurity vulnerabilities and threats;

The 44th Global Privacy Assembly therefore resolves to:

1. **Take steps to develop an understanding of the remits and responsibilities of GPA member authorities in relation to cybersecurity;**
2. **Explore possibilities for international cooperation, knowledge and information sharing, including technical expertise and best practices, amongst GPA members to avoid duplication in investigations or other regulatory activities regarding cybersecurity issues and regulatory approaches as they relate to data protection and privacy;**
3. **Request the GPA's International Enforcement Cooperation Working Group to deliver exploratory work by autumn 2023, taking account of the work carried out by other GPA Working Groups where relevant and consulting with the GPA Reference Panel as appropriate. The GPA should also determine whether to pursue the work under its next Strategic Plan from 2023.**
4. **Request the International Enforcement Cooperation Working Group to agree a workplan to deliver the steps above, focussed on clear and practical outcomes which should include delivery of a closed enforcement session on cybersecurity issues in 2023.**

Explanatory note

The increasing prevalence of cyber attacks across global regions requires a robust and coordinated regulatory response to protect individuals' personal data. State actors and non-State criminal entities pose threats in cyberspace evermore easily, partly due to the rapidly accelerated digital

interconnectedness of society since the COVID-19 pandemic emerged[4], but also due to supply chain vulnerabilities within final products. This resolution focuses on the mitigation and remediation of cyber attacks. GPA members have conducted significant volumes of cyber incident investigations involving discovery of serious mishandling of the most sensitive data categories, including gender reassignment, health data and physical identity (which could include race or ethnic origin, etc). The lack of security awareness in organisations, the lack of information security accountability, effective risk management and regular checks throughout the supply chain is often at issue.

Complex supplier ecosystems for delivery of services can mean greater risk of vulnerability, for example one supply chain attack at a single weak point generated by poor supply chain risk management can enable cyber attackers persistent access to many other servers globally over a sustained period. Individuals' money, personal data and information are at risk and their access to public and private sector services and knowledge significantly suffers as a result of these cyber threats.

Governments and regional authorities or groupings of governmental cooperation have reacted with new laws, policies and fact-finding initiatives to protect their critical national infrastructure, to safeguard their role in maintaining their public functions, and businesses' livelihoods fundamental to the health of national economies. Cybersecurity does not just entail a single factor for organisations; key factors such as data security, system security, online security and device security all require consideration to prevent harms occurring.

Governments continue to recognise the need to align data protection and network information systems and security law in order to provide a more comprehensive enforcement and prevention effort.

Developments in Europe and the Americas are just some of the recent general cybersecurity framework additions to the legal rulebooks and cooperation initiatives which have emerged in the past two years to build resilience, prevent unauthorised access to networks and enable recovery plans where attacks have been successful. This may include solutions such as Computer Security Incident Response Teams (CSIRTs), or establishing a competent national authority to issue guidance and manage information or security incidents.

Regional, national and local laws have required municipalities and other decision-making public authorities to significantly increase their resilience and some data protection and privacy authorities are already looking at ways they can assist in these efforts.

Inter-governmental entities like the OECD have recognised[5] the need to coordinate and better inform stakeholders throughout the supply chains to effectively address vulnerability threats, to better understand the position of security researchers, and to develop ways for good vulnerability management to be recognised as indicators of compliance with privacy legislation like the GDPR.

---

[4] For example, the UK National Cyber Security Centre (NCSC) reported in 2021 a threefold increase in ransomware incidents with government, companies and individuals being targeted in a more aggressive manner than previously seen: ISC-Annual-Report-2019–2021.pdf (independent.gov.uk)And for commercial sources: 2021_NCC_Group_Annual_Threat_Report.pdf Page 19.

[5] pdf (oecd.org) Working Party on Security in the Digital Economy – Report: Page 76, ENCOURAGING VULNERABILITY TREATMENT Responsible management, handling and disclosure of vulnerabilities, February 2021

Some of these needs have similarly been emphasised through several cross-country reports of regional organisations[6] like the European Union Agency for Cybersecurity (ENISA) or the Organisation of American States (OAS).

Data protection and privacy authorities can assist with guidance on legal compliance as well as what the new laws mean for better protection of personal data in the event of a cyber attack. There is nascent recognition of the partnerships that data protection and privacy authorities need to forge with domestic counterparts to provide a coordinated, strong, risk-based response against cyber threats. But partnerships with entities in other parts of the world to more effectively combat threats to individuals' personal data across borders and maintain cyberspace stability need to be considered too.

The Global Privacy Assembly (GPA) has started to look at isolated cybersecurity threats in more detail in recent years since the COVID-19 pandemic emerged, in particular looking at topics such as credential stuffing, and the way in which video teleconference companies (VTCs) can protect their users from threats to online meetings.

But the GPA can take action more broadly in relation to promoting and creating better understanding amongst its members about the range of cybersecurity harms, both individual and societal, drawing from recent research done by individual GPA members.

The GPA's 2021-2023 Strategic Implementation Plan has clearly mandated[7] its members to identify and consider topics of focus relating to surveillance of citizens and consumers in the digital economy, and for the International Enforcement Working Group and Digital Economy Working Group to lead this work, supported by others.

The GPA has also called[8] on its International Enforcement Working Group to continue monitoring for opportunities for enforcement cooperation, noting the new and emerging digital risks posed to individuals' privacy. The challenges outlined in this resolution would fall within this Strategic Plan's current mandate.

These activities outlined below should be considered and agreed by the International Enforcement Working Group for its 2023 workplan to result in clear and practical outcomes:

- The International Enforcement Working Group has evolved in recent years to develop its capability to run closed enforcement sessions, and currently, this Working Group is best placed to deliver exploratory work by 2023 on surveillance threats and harms for individuals and society.

- The Working Group would not work in isolation, rather taking account of relevant work carried out by other GPA Working Groups, such as that of the Digital Citizen and Consumer

[6] Coordinated Vulnerability Disclosure Policies in the EU — ENISA (europa.eu) ENISA, April 2022 and National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf (oas.org) OAS, June 2022

[7] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org) See page 16 in particular.

[8] As above, page 21.

Working Group's current consideration of other realms of cross-regulatory intersection, and consulting with the stakeholder reference panel as appropriate.

- The GPA should take initial efforts to explore cooperation opportunities in this field. There may be value in data protection and privacy authorities exchanging information to more effectively combat criminal cyber activity in relation to individuals' personal data. This may include exploring where common action can be taken to shine a light on the problems commonly faced simultaneously across jurisdictions. This will help avoid duplication of effort across GPA Members' investigations.

- The GPA could also, as appropriate, engage in information sharing and explore cooperation with regional and international organisations that address cybersecurity.

- The Assembly remains well placed to act based on past successful collaboration on isolated cyber-incident related matters outlined above. In this instance, the GPA could share experiences, or compare existing models to prevent, mitigate or avoid the harms generated by cyber threats, thereby contributing to cybersecurity capacity building at the national level. The GPA may also assist with leveraging the technical skillset of the larger authorities to the benefit of those members with fewer resources available for this field of activity.

This international cooperation work by the GPA may help protect individuals in multiple jurisdictions from economic and psychological harms. It may also support domestic efforts in advising organisations in the advent of ransomware attacks, for example where organisations are locked out from their own data until a monetary sum is paid, or other serious economic consequences of supply-chain attacks.

The GPA should determine at the Closed Session in 2023 whether to pursue further work on cybersecurity and related surveillance threats and harms. It should draw from the basis of exploratory work done in 2022 pursuant to this Resolution. Any further work would proceed under the next GPA Strategic Plan due to be adopted in 2023.

END