COVID-19 Protocols Lessons Learned Survey Results Report

Executive Summary of Survey

As part of the response to COVID-19 protocols implementation, a significant amount of personal data and special category data, namely personal health information, has been collected and shared by our employers, businesses, schools, insurance companies, healthcare providers and government agencies. In order to properly understand how well-equipped these organizations were for handling personal data in volumes and ways they have not experienced before, the GPA COVID-19 Working Group surveyed non-privacy regulators, individuals and organizations about the information they provided along with the COVID-19 data collection protocols regarding how to collect it, process it, store it, and share it. The survey set about understanding what data protection authorities or similar regulators could have done better and what they did right. These lessons learned will then be reflected potentially in COVID-19 Working Group guidance, the 2nd edition of the Compendium on Best Practices that Sub-group 1 on Emerging Issues has compiled, and as best practices and suggestions for GPA Members and Observers to issue via their own supervision, guidance and outreach methods.

The resulting lessons learned, set out below the detailed analysis of each thematic area, capture options for regulatory capacity building within the specific context emergency regulatory response, COVID-19 or otherwise. As this is the first major, global emergency scenario in the era of data protection and digital footprint of individuals and governments, it has shown a light on the need to develop an "Incident Response" toolkit for regulators, as well as other ways privacy regulators in particular may take a leading role in such response, given the criticality of the data collected and associated risks.

Main Thematic Areas Reviewed in the Survey

1. Communications and guidance (Q 1 to 5)
2. Organizational / operational impact of COVID-19 19 restrictions on data subjects' rights (Q6 and 7, 16 to 20)
3. Sharing, Security and breach reporting (Q10 to 14, Q26 to 30)
4. Privacy Tech / IT Development, framework and design (Q20 to 24)
5. Supervision and Enforcement (Q8, 9, 15 and 25)

Survey link: https://survey.alchemer.com/s3/6191656/Global-Privacy-Assembly

Responses and Analysis

1. Communications and Guidance

Overall, regardless of the existence of data protection and privacy laws in the jurisdiction, respondents indicated that additional guidance and clear, consistent implementation measures across all regulators, privacy and non-privacy, would be useful to them. Some suggestions included:

a. providing a holistic document to guide all aspects of not only data protection, security, retention and sharing during in an emergency such as the COVID-19 pandemic, but the larger impact on business / business impact of data breaches;
b. better use of social media to share messaging;
c. checklists with clear instructions for all entities that had to implement new / update old measures; and
d. earlier, more targeted responses

Respondents suggested that the privacy regulators should have more decision-making authority and involvement in the pandemic response protocols. Also, small and medium enterprises with already limited resources, that were then negatively impacted by lock down and the resulting economic downturn, requested additional resources to help decision making. A very clear concern was echoed throughout, regarding online fraud and phishing attacks. One responded stated, "Intensify the fight against the growing number of online fraudsters… exploiting the public fear surrounding the COVID-19, using the pandemic to lure people into clicking phishing emails and installing malware capable of stealing personal data and money."

Lessons Learned:

A coordinated, cross-disciplinary guidance document showing the links between specific regulatory objectives and the underlying privacy and security concerns is needed. Health, education, economic and social objectives in preventing the spread of COVID-19 all have privacy and security issues attached to them, presenting issues that were probably already existing but now have come to light. There is an opportunity to re-visit and improve the way data is managed. Regulatory capacity across all relevant regulators in pandemic / emergency response should be built. When the situation returns to a bit more normal, this collaboration should continue, to build guidance and an emergency incident response plan comprising all facets of regulatory impact: privacy, yes, but also health care, economic / financial, education and other relevant stakeholders.

2. Organizational / operational impact of COVID-19 restrictions on data subjects' rights

While data collection and processing changed in that certain types of sensitive personal data were being collected on a much larger scale, generally it appears that little else changed in that regard. The main change in data collection by organizations at the request of health regulator response requirements was around an increase in health data collection (temperature taking, COVID-19 test results, vaccination records, etc), which should come as no surprise. Respondents clearly indicated by an overwhelming

majority response that data subjects' rights have always and continue to be very important to them within their organizations. A small number of respondents developed new policies and procedures, presumably where none existed before, as a result of COVID-19 response requirements. Some changes were made, but in large part privacy and security policies and procedures remained unchanged. The primary types of safeguards and controls that most respondents supported were based on developing relevant contractual clauses or data processing agreement in order to manage privacy and security requirements.

Lessons Learned:

Regulators should push entities to prioritize policy and procedural reviews due to the increase in a specific type of data collection, i.e., health data. Entities that never collected such data before must have a clear directive about how to collect it and what to do with it once they have it, from sharing to storing to deleting (if ever). Additional types of safeguards may need to be developed as well for processing, as contractual clauses, DPAs and even consent may not be enough to ensure it is managed properly. Work with each other and with other regulators to brainstorm what other safeguards may work to protect such data. Perhaps for example regular technical reviews and audits should be documented on at least an annual basis and spot checked by each regulator on an appropriate scale.

3. Sharing, Security and Breach Reporting

Understandably, government data sharing requests increased quite a bit during 2020, as health and education regulators and facilities sought to learn about who, where and why people were getting infected with COVID-19. Where data sharing requests were made, the purpose and scope of the requests were clear and specific, and the requesting authority, where applicable, was happy to apply appropriate safeguards and controls to the transfers. Most data sharing requests were from either the local health or public safety regulators. Note well, in any case, that over 60% of respondents did not attempt to suggest to the government requesting authority that any controls be applied to the data sharing.

Interestingly, while a small majority of respondents were concerned about enforcement action as a result of privacy issues around COVID-19 response data collection and processing, a large majority thought that nothing should change in terms of privacy and security enforcement action, which, as suggested in the survey, is a key learning tool.

Lessons Learned:

Even before COVID-19, data sharing requests from government agencies posed privacy and security concerns. The pandemic highlighted, however, the need for guidance or perhaps incorporating into legislation the requirement to insist on controls and safeguards specifically where government data

sharing requests are made, including contractual clauses accounting for the innate conflict that often exists between public safety and national security objectives and protecting personal data. Very often contractual clauses meet tick box requirements and are much too general to adequately address this conflict. Compliance with laws clauses, as well as "public interest" legislative requirements, potentially weaken the ability to sufficiently protect personal data. A set of government data sharing policies, procedures and contractual clauses, both general and COVID-19 specific, could be developed to address such concerns.

4. Privacy Tech / IT Development, framework and design

Perhaps unsurprisingly, most respondents said that they are using privacy enhancing technology (PET) such as encryption and two factor authentication in their IT infrastructure. A small percentage are using anonymization/pseudonymization tools or digital signatures. Nearly all respondent jurisdictions have contact tracing apps that are not mandatory to download or use but are user friendly.

Lessons Learned:

Informational fact sheets and other clear, understandable templates and tools may be developed about incorporating PET, privacy engineering and innovative ways to better protect specific data types, such as data collected in response to or as a result of emergency conditions. A playbook for pandemics / emergencies would be useful as well, as part of national planning for emergency response and / or business continuity with respect to IT, security and data protection business critical risks, especially where they all cross over with each other. Keeping a risk register updated with data protection related risks is underrated and underdeveloped in certain regions, as this area of IT compliance and governance still develops. Targeted, instructional information sharing from regulators on a campaign level basis to assist with risk reporting is critical to the success of any enhanced PET or other types of privacy by design for an emergency. Updating privacy laws or creating regulations to address PET use and bare minimum standards may also be helpful in ensuring this area of response requirements and controls is taken into account.

5. Supervision and Enforcement

Generally, the respondents agree that the development of COVID-19 and contact tracing apps are important to develop, and at the same time, innovation in developing them can co-exist with strict privacy compliance and oversight. Most of them also thought that supervision and enforcement should be conducted as usual. There was a reasonably moderate percentage that suggested privacy regulation should be flexible thereby allowing for innovation. Based on experience of the past year, most respondents wanted supervision, outreach and training on Security measures for managing COVID-19 restrictions and data sharing requirements, especially where working from home is necessary. Others indicated they want support in understanding any new or revised guidance on breach reporting during a

pandemic, i.e., what is a breach in the new processing environment we find ourselves in, has anything changed, what new factors should be considered, etc.

Lessons Learned:

Developing a better understanding of the impact and transparency about data management and sharing through COVID-19-specific privacy notices may affect how organizations assess the risk and requirement around breach reporting. Regulators can provide guidance about what issues in such an emergency situation should be clarified to data subjects with respect to data collection and processing during an emergency response period, what regulatory obligations they are subject to, and any other templates for business-critical response controls should be considered.

Conclusions:

While the COVID-19 pandemic continues to be hard fought, personal data remains at risk as tools are developed and gains are made to improve public health and travel at the cost of privacy and potentially security. More information must be collected, some that never existed before or if it did, it was very sensitive, for example medical and health related data that only medical professionals and hospitals had access to. Where more information is collected and processed, risk increases, and additional work must be done to understand new and innovative ways of protecting privacy as well as the risks involved. Ethics becomes even more important, and we as regulators must continue to ask ourselves what we are learning along the way, are we addressing the appropriate issues, and what practically can be done. For future lessons learned surveys, we may consider more nuanced themes, such as:

- ✓ What are the ethical issues around data sharing for the public good (both about sharing and about not sharing data, when is it appropriate, who decides, etc). The concept of "the public good" indicates almost an *imperative* to share data, but it may simply not be feasible or a data subject may strenuously object to it… who wins? What is truly the right thing to do? What if it means retaliation, exclusion, or worse? Could these issues be the result whether the data is shared or not, i.e., the proverbial rock and a hard place? If I share I'm excluded because I have COVID-19, or haven't been vaccinated / don't have an acceptable "standard" record, etc. The GPA COVID-19 Working Group is preparing a resolution on this matter, draft is pending and may be the subject of another, follow up webinar.

- ✓ While data protection and privacy laws and principles are largely about accountability, and making a risk based self-assessment about processing personal data, are there any specific, absolute do's and don'ts for organizations and individuals to follow? Can we as regulators do more to provide clear starting points and specific guidance as subject matter experts calling on people with perhaps less expertise to make some very difficult calls?

- ✓ During a pandemic, does all data sharing simply become high risk processing, such that, at least temporarily, a Data Protection Officer (DPO) or some other role of accountability in any organization, big or small or otherwise, should be appointed? Is this something that becomes part of any national emergency response protocols, required by laws or regulations for example?

The GPA COVID-19 Working Group continues its work to better understand and even get ahead of such issues to help better enable data protection and security at any given time, and for any entity collecting and processing personal data, especially in such precarious times.