Global Frameworks and Standards Working Group

Report – August 2023

Chair authority: UK Information Commissioner's Office

Table of Contents

Executive Summary

The Global Frameworks and Standards Working Group (GFSWG) has made good progress in 2022-23 in contributing towards the delivery of the GPA's strategic priorities and plan.

Building on our earlier analytical reports[1] on global data protection frameworks and cross border transfers, we have completed our work to provide the GPA with a collective global statement on high data protection and privacy standards. We have also continued to support cross border data flows by producing a detailed comparison of standard contractual clauses across several frameworks and jurisdictions, to assist GPA members and organisations in their jurisdictions in their understanding of different transfer mechanisms.

High standards of data protection and privacy

In 2022-23 we have completed our allocated action from the GPA's Strategic Plan 2021-23[2] to work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards. This goes to the core of the GPA's work - setting out a common view on high standards will support regulatory cooperation, as well as promote high standards globally and influence discussions in a consistent way, both internationally and within GPA member jurisdictions. We have prepared a resolution which sets out a collective global statement by data protection and privacy authorities on the high level principles we consider important to achieve high data protection standards. We will submit that resolution for adoption at the GPA 2023 in Bermuda.

Cross border transfers and mechanisms

In line with GPA's strategic priorities, the GFSWG recognises the importance of protecting personal data wherever it flows as the global digital economy continues to develop, and we have continued to work on this topic in 2022-23 to support the secure and smooth flow of personal data across borders. Our work has continued with an intention to assist GPA members and organisations in their jurisdictions in their understanding of different transfer mechanisms, and has this year focused on developing a detailed comparison of standard contractual clauses across several jurisdictions and frameworks.

The GFSWG is pleased to submit its annual report, and other outputs from the above work items in annexes, for adoption by the Closed Session.

[1] In 2020: Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf (globalprivacyassembly.org) and 2021: 1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf (globalprivacyassembly.org)

[2] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)

Introduction

Global frameworks and standards are a vital element of the GPA's first strategic priority – to advance global privacy in an age of accelerated digitalisation, as the GPA continues to work towards a global regulatory environment with clear and consistently high standards of data protection. Global frameworks and standards have an important role to play in promoting consistently high standards of data protection and privacy globally – increasingly so as more jurisdictions adopt new data protection and privacy laws, and review existing ones, every year. Additionally, as the global digital economy grows, so does the volume of data processed, both within and across jurisdictions. The GPA's work on global frameworks and standards to date has identified elements of convergence which can foster interoperability, and support the trusted flow of data across borders.

The Global Frameworks and Standards Working Group (GFSWG) is now in its fourth year of operation. Its current mandate can be found in the adopted Resolution on the Assembly's Strategic Direction 2021-23[3], which includes specific actions for the GFSWG to deliver by October 2023.

In its first year of operation the GFSWG delivered a wide-ranging comparative analysis of ten global and regional data protection and privacy frameworks, which highlighted a high degree of commonality between their core principles, rights, and general approaches to accountability and cross border transfers and suggested that shared values exist between the frameworks and between the jurisdictions in which they apply. We followed this with a comparative analysis of cross border transfer tools and mechanisms across the ten global frameworks, and found substantial commonality between the frameworks in the tools that existed within them to enable transfers, but some difference in the detail, and in the way they were implemented.

The GFSWG's work in 2022-23 has built on those earlier comparative analyses, with two main objectives – firstly, to harness the apparent commonality and shared values between jurisdictions identified in earlier work to produce a resolution on agreed principles for high data protection and privacy standards across the GPA membership, and secondly, to assist GPA members and organisations in their jurisdictions in their understanding of different transfer mechanisms.

The GFSWG has therefore worked on the following items in 2022-23:

- **Work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards.**

A common view of what is meant by high data protection and privacy standards can support regulatory cooperation, so is at the core of much of the GPA's work. In 2023 the GFSWG continued the foundational work to understand what that common view might look like. This included carrying out a GPA member survey, which led to the drafting of a resolution setting out the core principles, rights and other elements that GPA members would

[3] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)

advocate for. That resolution is being submitted for adoption at the GPA conference in Bermuda in October 2023.

- **Continue work on cross border transfer mechanisms**

Cross border transfers continues to be a very relevant topic. The need to protect personal data wherever it flows continues to be vitally important as increased digitalisation results in higher volumes of personal data being processed in the global digital economy, and the GFSWG continues to be keen to do what it can to support the secure and smooth flow of personal data across borders.

To date the GFSWG has delivered various comparative and analytical outputs, including a high-level analysis and report on transfer mechanisms in 2021. Our outputs to date have focused on clarifying understanding of transfer mechanisms in various global frameworks, and have highlighted commonality between them. This in turn has supported wider work carried out by organisations such as the G7 and OECD on Data Free Flow with Trust (DFFT).

In 2023 our work on cross border transfers focused on explaining transfer mechanisms in more detail, and WG members have completed a detailed comparison of standard contractual clauses in different data protection frameworks (ASEAN; Council of Europe; EU; RIPD (Ibero-American Network); Argentina; New Zealand and UK;). This work is aimed at helping GPA members and organisations in their understanding of different transfer mechanisms.

- **Develop formalised relationships with other fora undertaking similar work, taking into account work done by SDSC on stakeholder engagement where appropriate.**

The GFSWG is fortunate to have observers to the working group from various other bodies and fora, such as the OECD and Council of Europe. The WG is also fortunate to have several members with close links to the G7 and its Roundtable of Data Protection and Privacy Authorities. This has allowed us to engage with stakeholders working on similar issues to consider where our work aligns, and to ensure that our work is complementary and not duplicative.

More detail in relation to the above work items, including further reports and outputs can be found in the next section and in annexes to this report.

Finally, the GFSWG Chair's representative attended several 'deep dive' meetings with the GPA ExCo's Strategic Direction Sub-Committee (SDSC) in 2023. During these meetings, presentations were made to SDSC on progress made, questions answered and feedback received.

Working Group members

UK ICO (Chair)	OPC Canada	Côte d'Ivoire	Council of Europe DPC
Dubai IFC	EDPS	CNIL France	Gabon
Germany BfDI	Israel	PPC Japan	Kenya ODPC
Korea PIPC	INAI Mexico	OPC New Zealand	Peru
NPC Philippines	Portugal	San Marino	Senegal
Spain	Switzerland FDPIC	KVKK Turkey	US FTC
Uruguay	European Commission (observer)	European Data Protection Board (observer)	OECD (observer)
New York City Office of Information Privacy (observer)	Chief Privacy and Civil Liberties Officer, US Department of Justice (observer)		

Working Group Activities

The GFSWG's activities in 2022-23 have centred around the work items listed above in the introduction section. In more detail, those activities have included:

- **Work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards.**

The GPA Global Frameworks and Standards Working Group (GFSWG) was allocated an action in the GPA's Strategic Plan 2021- 23 to "work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards". This goes to the core of the GPA's work, both in the context of the GPA mission - where one element is to provide regulatory and policy leadership at the international level in data protection and privacy – and in the GPA's first strategic priority, which commits us to "work towards a global regulatory environment with clear and consistently high standards of data protection, as digitalisation continues at pace". The intention is that by adopting a resolution or policy statement on the GPA member authorities' common view of high data protection and privacy standards, the GPA will advocate for and promote high standards globally and within member jurisdictions, which in turn can support the protection of personal data wherever it flows.

The GPA last set out its views on high *general* data protection and privacy standards (as opposed to high standards in relation to particular activities) in 2009, in the Madrid Resolution[4]. As a starting point, the GFSWG reviewed that Resolution. We found that many of the principles, rights and other elements in the Resolution remain familiar today - for example key principles are covered, several accountability measures are included, and the importance of an independent and impartial supervisory authority is emphasised.

However we also noted that in the 14 years since the Madrid Resolution was adopted, there have been (and continue to be) huge and rapid, ongoing changes as the global economy and society has become increasingly digitalised; data protection laws and frameworks have developed and been updated; and regulatory authorities have also evolved. We therefore wanted to understand which principles, rights and other elements GPA members would agree were important to advocate for now, to ensure high global data protection standards.

We therefore developed a GPA member survey, based on the principles, rights and other elements in the Madrid Resolution and with the addition of others from more recently-adopted instruments, to understand what authorities consider as important now – and what will be important to make today's data protection frameworks fit for the future.

The survey included questions on whether those principles, rights and other elements were relevant; whether they needed emphasising; whether current legislation in member jurisdictions reflected similar content; whether members were calling for legislative change

[4] 14302 STANDARDS.qxp:Maquetación 1 (globalprivacyassembly.org)

in their jurisdiction, and what other principles, rights and other factors should be included. The survey summary report can be found in annex A.

Survey responses indicated that a resolution would be a helpful mechanism for the GPA to use to advocate for those principles, rights and other elements to achieve high global data protection and privacy standards, and to call for law and policymakers to use the expertise of data protection and privacy authorities as they develop and implement new laws and policies. The resolution therefore sets out at a high level current expectations of the principles, rights and other important elements that are important to ensure high data protection and privacy standards in 2023, and which we would advocate for policymakers to consider including as their jurisdictions' laws are introduced and revised. The draft resolution will be submitted for adoption at the GPA 2023.

- **Continue work on cross border transfer mechanisms**

Cross border transfers is an increasingly relevant topic. The need to protect personal data wherever it flows continues to be vitally important as increased digitalisation results in higher volumes of personal data being processed in the global digital economy. There is an increasing number of transfer tools and mechanisms being developed across different jurisdictions and frameworks, providing reassurance that personal data can be appropriately protected across borders, but also the potential for complexity which organisations transferring data can find difficult to navigate.

Through our literature review carried out in 2022[5] and ongoing informal monitoring we are acutely aware that there are a variety of projects being undertaken by international bodies and fora, networks and individual jurisdictions and organisations to support cross border transfers[6], such as the work to develop and operationalise Data Free Flow with Trust (DFFT) by the G7 and its Roundtable of Data Protection and Privacy Authorities, and the OECD.

The GFSWG continues to be keen to do what we can to support the secure and smooth flow of personal data across borders. Findings from the 2022 literature review indicated that there were opportunities for further GPA work on this topic, which could aim to:

- aid further understanding of current and emerging transfer mechanisms;
- highlight commonality and convergence;
- monitor developments; and
- foster engagement with global networks, multilateral organisations and other key stakeholders in order to support the above opportunities.

In 2023, GFSWG members have completed a detailed comparison of contractual clauses in the ASEAN, Council of Europe, EU, RIPD (Ibero-American Network), Argentina, New Zealand and UK. The contractual clause mechanism was chosen for the comparative exercise

[5] 2.2.b.-Global-Frameworks-and-Standards-Workin-Group-English.pdf (globalprivacyassembly.org)
[6] Some other examples (not exhaustive) – individual jurisdictions such as DIFC: Data Export & Sharing | DIFC; regional networks such as ASEAN/European Commission: (Final) Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf (europa.eu)

because contractual clauses have been identified as one of the more prominent mechanisms across the regions of the GPA.

Controller-to-controller and controller-to-processor clauses have been included, with a separate comparative table for each. The tables are intended to provide a comparative tool for organisations using contractual clauses for data transfers.

The tables can be found at annexes B and C, in the accompanying documents.

Forward looking plan 2023-2024

At the time of writing, the current GPA Strategic Plan 2021-23[7] notes the importance of promoting high standards of data protection and privacy, the need for mechanisms to ensure that personal data is protected wherever it is processed, and the role the GPA can play in doing this.

The GPA will adopt a new Strategic Plan in 2023 for the 2023-25 period. This means that the proposals for the GFSWG forward looking plan for 2023-24 will need to be aligned with that overarching plan, so until it is adopted the proposals in this section are provisional.

The GFSWG proposes to work on the following items:

- **Promoting high standards of data protection and privacy**

If the high standards resolution is adopted by the GPA membership in October 2023, the GFSWG will need to consider how and where to promote it, both among GPA members so that they implement the resolution by advocating for the adopted principles in the resolution in their respective jurisdictions, but also externally to raise awareness among law and policymakers.

- **Cross border transfers and mechanisms**

The GFSWG should consider carrying out further work on cross border transfers in 2023-25, although we should ensure it complements and does not overlap the work already being carried out by other international organisations (particularly the G7 and OECD work to develop and operationalise Data Free Flow with Trust), and by non-GPA data protection authorities, regional or other fora.

The comparative analysis on contractual clauses should be promoted as appropriate.

To understand where the GPA can best add value to the global conversation on transfers, it would be helpful to first understand any particular needs or concerns that GPA members (and organisations in their jurisdictions) have relating to transfers. The current regulatory landscape, as well as current issues, needs and concerns could be identified by carrying out a GPA member survey, with a view to better understanding but also to explore whether the GPA can undertake practical activities to support authorities on this issue.

Other activities to consider could include other comparative analyses, on different transfer mechanisms, and external engagement with others working on cross border transfers.

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

Conclusion

In 2022-23, the GFSWG has made good progress against our work plan and actions allocated to us by the GPA Strategic Plan 2021-23. We have:

- Completed the GPA's work on global data protection and privacy frameworks, culminating in our draft resolution on high data protection and standards. If adopted, this will provide the GPA with a collective global statement by data protection and privacy authorities on the high level principles we consider important to achieve high data protection standards. That statement will aim to influence discussions in a consistent way, both at international level and with relevant policy makers within individual GPA members' jurisdictions.

- Carried out further work on cross border transfers and mechanisms, in the form of a detailed, comparative piece of work on contractual clauses. The tables are intended to provide a comparative tool for organisations using contractual clauses for data transfers.

As global frameworks and standards continues to be a crucial element of the GPA's work towards a global regulatory environment with clear and consistently high standards of data protection, we look forward to continuing with our work in 2023-24.

The GFSWG Chair would like thank the members and observers of the Working Group, and in particular those who have worked within the sub groups, for their contributions this year.

Annexes

Annex A: GPA member survey on the GPA's view of high data protection and privacy standards – report

GPA Global Frameworks and Standards Working Group

GPA member survey on the GPA's view of high data protection and privacy standards – report

1. Background

The GPA Global Frameworks and Standards Working Group (GFSWG) was allocated an action in the GPA's Strategic Plan 2021- 23 to "work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards". This goes to the core of the GPA's work, both in the context of the GPA mission - where one element is to provide regulatory and policy leadership at the international level in data protection and privacy – and in the GPA's first strategic priority, which commits us to "work towards a global regulatory environment with clear and consistently high standards of data protection, as digitalisation continues at pace". The intention is that by adopting a resolution or policy statement on the GPA member authorities' common view of high data protection and privacy standards, the GPA will advocate for and promote high standards globally, which in turn can support the protection of personal data wherever it flows.

The GPA last set out its views on high *general* data protection and privacy standards (as opposed to high standards in relation to particular activities) in 2009, in the Madrid Resolution. As a starting point, the GFSWG reviewed that Resolution. We found that it appears to be quite comprehensive and forward-thinking for its time, as it includes some important provisions that would still be agreed today as exemplifying high standards – for example key principles are covered, accountability measures included, and the importance of an independent and impartial supervisory authority is emphasised. The resolution also includes a clear expectation that principles and rights should only be restricted by states when necessary and only in certain circumstances, as provided for by national legislation which establishes appropriate guarantees and limits on such restrictions to preserve individuals' rights.

However we recognise that in the 13 years since the Madrid Resolution was adopted, there have been huge and rapid, ongoing changes as the global economy and society has become increasingly digitalised; data protection laws and frameworks have developed and been updated; and regulatory authorities have also evolved. Those changes continue, as new, data-driven technologies emerge and rapidly evolve with the potential to transform the way in which we live and work, bringing with them opportunities to improve our lives but also presenting privacy and data protection risks which must be addressed.

2. Survey aims and methodology

We developed a GPA member survey to understand whether today's member authorities of the GPA consider the principles, rights and other elements in the Madrid Resolution still relevant. We also wanted to understand whether members thought that the GPA should re-emphasise the importance of those core elements of the Madrid Resolution, as well as what additional principles, rights and other elements authorities consider as important now – and what will be important to make today's data protection frameworks fit for the future.

The survey therefore included questions on:

- Whether each of the principles, rights and other elements of the Madrid Resolution were still relevant;
- Whether they needed stronger emphasis, and whether this should be done in a new resolution / policy statement;
- Whether current legislation in the members' jurisdictions reflected those principles;
- Whether the member authority was currently calling for legislative change in their jurisdiction, and what they were calling for;
- What additional principles, rights, other factors should be included – that members would wish to advocate for as important for high data protection and privacy standards;
- Member authority current priorities, and current approach to cooperation and consultation to support, promote and achieve high standards; and
- Which organisations are best placed to take forward work to achieve high standards.

The survey used various forms of question – with some questions asking for simple yes/no/not sure responses, and others allowing for respondents to rate their level of support on a more granular level for additional principles, rights and other elements - using strongly support/support/less strongly support/do not support/not sure responses. This was to ensure that levels of support for the GPA advocating for additional elements could be analysed in more detail. All questions also allowed for free comments to be noted. In this way we aimed to obtain a baseline of quantitative data, but substantially backed up by qualitative comments.

3. Survey results

27 responses to the survey were received, covering most regions of the GPA: three from Asia, 17 from Europe, two from North America, four from South America and one from Oceania.

3.1 Relevance of principles, rights and other elements in the Madrid Resolution

As might have been expected, over 80% of responses agreed that all principles, rights and other elements in the Madrid Resolution were still relevant.

Most responses also agreed that most of the principles, rights and other elements in Madrid needed stronger emphasis. A substantial number of responses noted similar reasons for this, some highlights of which included:

- New technologies can enable large volumes of data to be processed and shared for purposes that are sometimes different and unexpected.
- The **principle of data minimisation** was noted as being implied by the Proportionality principle in Article 8 of the Madrid Resolution, but as fundamentally important and as such should be explicitly included and emphasised. It was noted that the wording of Article 8 where it states that "reasonable efforts" should be made to limit processing to the minimum necessary, was no longer appropriate and should be strengthened.
- **Proportionality** was noted as a key principle that should be emphasised in a broader sense than Article 8, in order to respond to newer types of processing, such as facial recognition technologies and biometrics, where the proportionality of the processing operation in relation to the purposes is a key element to address.
- The **principle of data quality** was highlighted as being increasingly important – with the risk of significant decisions about individuals being incorrectly made being exacerbated by the use of automated processing / decisions and artificial intelligence (AI). The serious implications of this for decisions relating to finance, research and criminal offences were mentioned. The importance of data quality in training AI systems to prevent bias and discrimination was also noted.
- Responses emphasised the importance of **transparency** for processing in the digital economy – in terms of ease of understanding, accessibility and provision of clear information on the processing and on people's rights. Some caution was noted on over-reliance on notice and consent mechanisms over other principles, and that an explicit right to be informed was also desirable.
- Having an **accountability principle** was agreed to be important, though it was noted that this **should be accompanied by other practical elements** to operationalise it, such as privacy by design, data protection / privacy impact assessments, privacy management programmes and data protection officers.
- Almost all responses agreed that **sensitive / special category data** was highly important, and a large majority agreed the need to emphasise it and to include extra safeguards. There was some variation in what did, and should, constitute sensitive data – with notable comments about adding biometric, genetic and neurodata to this category where it did not already feature.
- Almost all responses noted the relevance of **international transfer provisions**, and 67% wanted to see more emphasis in this area. Businesses and individuals were noted as needing clear and simple global principles and mechanisms to protect data as it flows. Other comments said specific mechanisms should be referred to and highlighted, and that elements of data free flow with trust (DFFT) should be included, in terms of the coexistence and interoperability of various transfer tools, and the importance of providing multiple options for businesses. One comment suggested a new approach to international transfer tools was needed.
- Again, almost all responses agreed that the existing rights in Madrid were still relevant, with many also agreeing that more emphasis was required. Several comments suggested that **rights should be expanded or otherwise framed to**

include AI processing and automated decisions, while others focused on the need to ensure that timeframes for organisations to allow individuals to exercise their rights were clearly set out. The need to align with modern instruments such as Convention 108+ was also noted.

- **Security provisions** were seen to be very important, with almost all agreeing their relevance and 70% also agreeing that more emphasis was needed. Heightened security risks from technical advances, increased participation in the digital environment, increased cybersecurity risks were all highlighted in comments. Other comments suggested a need for **mandatory breach notification**, as well as the need to ensure complementary legislation and regulation on related areas such as cybersecurity.
- Linking in with the accountability principle above, almost all respondents agreed that **proactive compliance and monitoring measures** were relevant, and two-thirds agreed that they needed more emphasis. A variety of comments were offered, which included:
    - that measures should be appropriate to risk;
    - that modern frameworks tended to include these measures, sometimes as legal obligations;
    - that privacy impact / risk assessment was especially important in developing and implementing new technologies;
    - that audits and vulnerability testing of IT systems could be specifically referenced, given the growing digital economy; and
    - that a well-resourced supervisory authority was needed to ensure that measures were properly implemented.
- **Cooperation** was also highlighted as relevant and increasingly important, with comments noting the need for authority cooperation as data flows across borders. Benefits of cooperation were noted, such as efficiency as limited resources could be pooled, increased knowledge, reduced duplication, and the enhanced impact of a shared voice. Greater consistency across jurisdictions was also noted, which could improve ease of compliance for organisations. Cooperation on breach responses was also noted as important and helpful.
- Most respondents also agreed the continued importance of having an appropriate **liability** framework in place – involving controllers, processors in sole and joint roles as per the circumstances of the processing. This links in with, and can be supported by, supervisory authorities having sufficient resources and powers to ensure effective investigations to establish liability, and appropriate enforcement action to be taken. Authority resources and powers were noted by several respondents as important to ensure high standards.

Over 90% of respondents agreed that current legislation in their jurisdiction generally reflected the Madrid principles, though some differences were noted – with some authorities reporting stronger provisions currently in existence, and others weaker ones. Approximately half of respondents said they were currently calling for changes to data protection and privacy laws in their respective jurisdictions.

3.2 Should the GPA re-emphasise the Madrid principles in a new resolution or policy statement?

All responses except one agreed that the GPA should re-emphasise the Madrid principles in a new resolution or policy statement, with just one replying with 'not sure'. Comments indicated that this related to the need to assess other competing GPA priorities, while still agreeing in principle that re-emphasising the principles would be a good idea.

Several responses noted in comments the need to better convey, and enhance, the principles to reflect today's digital economy in light of new challenges and technologies, and of new and updated instruments such as GDPR and Convention 108+.

3.3 Which additional principles, rights and other elements should also be included?

The survey suggested a list of likely additional principles, rights and other elements that member authorities might agree needed to be promoted as additional factors to achieve or support high data protection and privacy standards. There was also an opportunity for respondents to note any other elements they thought should be added.

- Over 90% of responses agreed that rights and safeguards relating to automated decisions should be included, with most respondents selecting 'strongly support'. Comments focused on the increased risk and impact on individuals presented by automated decisions, and that stricter safeguards relating to, for example, human intervention and transparency (on the existence of the processing, the logic involved, the significance of the consequences of the processing) should be highlighted. One comment noted that issues around automated decisions go beyond privacy to fairness and human rights, and that some such decisions could comply with privacy laws but still be harmful to individuals. The need to align with Convention 108+ and other modern instruments was again noted.
- Portability rights were less unanimously supported - although two-thirds of responses supported their inclusion, only a few 'strongly' supported it. However, it was noted that portability rights enhance the key principle of access, and was of increasing relevance in supporting individuals to have greater choice and control over their personal data.
- A right to restriction of processing was well-supported (85% supported or strongly supported it) however few comments as to why were offered, and there seemed to be some difference in understanding what such a right entails.
- 85% supported or strongly supported stronger protections for children and / or vulnerable people. Issues around children's data were noted to exit as more children connect online for education or social activities. Challenges such as obtaining meaningful consent, power imbalances and when parental consent might be needed were highlighted, as well as the need to educate and raise awareness of online risks. Marketing and profiling were also raised as issues to address. In addition to children,

vulnerable adults such as disabled people, migrants and older people were highlighted.

- Stronger emphasis on privacy by design and default was supported or strongly supported by 93% of respondents. Comments noted that although it was an established measure that supports responsible privacy development in products, services and business models, it is not a feature of all privacy and data protection laws, though some authorities in such jurisdictions include it in good practice guidance. New technological developments and possibilities made emphasising privacy by design and default increasingly important, with AI, biometrics, blockchain, the metaverse and robotics in healthcare all noted as developments that pose risks and could cause privacy and data protection harms if not developed with privacy considerations at the fore.
- Referencing a GPA position to access by third country authorities was supported or strongly supported by 74% of respondents. Comments highlighted the current emphasis on DFFT in several international organisations and fora and its increasing prominence as an issue to address. It was suggested that any GPA output refer to the principles set out in the OECD Declaration on Government Access to Personal Data held by Private Sector Entities and the GPA Resolution on Government Access to Data, Privacy and the Rule of Law.
- 85% of respondents supported or strongly supported the addition of cross-regulatory cooperation. Comments noted the increase in intersection between privacy and other regulatory spheres – competition, consumer protection, finance, telecoms, human rights. It was also noted that lack of cooperation risks duplication, outcomes that are not holistic and even conflicting, and that are not informed by the relevant regulator. On the plus side, cross-regulatory cooperation supported a coordinated and efficient approach to regulation.
- Two-thirds of respondents supported or strongly supported the notion of preventing harms. Comments, however, were varied. It was noted that the identification and prevention of harms was a key issue to include in a privacy management programme, and that it was a vital element of privacy protection, to consider not just individual complaints but broader societal harms. However, caution was urged that harms should not be a condition for privacy protection, or to exercise individual rights.
- Two-thirds of respondents also supported the notion of enabling responsible innovation. Again, comments were varied as respondents noted that it was vital in the current digital economy to respect fundamental rights and freedoms, and that the development of innovative technologies should do so. This would help build trust and further enable development. It was noted that innovation typically exceeds and outstrips privacy laws and oversight so it was important to address. Several comments focused on the importance of privacy by design and default – which are not typically the focus of technology development teams - in addressing this. It was noted by some that while this was a benefit of privacy by design, enabling responsible innovation was not in itself a supervisory authority's main focus. Finally,

it was noted that innovation could develop tools to achieve high standards of privacy and data protection, such as privacy enhancing technologies (PETs).

- Supporting economic growth, while recognised as a possible benefit of responsible innovation, was supported by less than 50% of respondents and comments noted that in itself it was not a factor contributing to high data protection standards.
- 75% of respondents supported or strongly supported data ethics as relevant in supporting high data protection standards. Comments noted that was particularly the case when considering innovative practices such as AI and automated decision making, the metaverse and blockchain, and the use of personal data in research, and for electoral purposes. However, it was cautioned that privacy as a fundamental right was a more relevant and important factor than ethics.
- As mentioned above, respondents were also given the opportunity to highlight other elements that they considered important to achieving or supporting high data protection standards. Specific mention was given to:
    - A right to be informed – beyond transparency and fairness, this was a key element to the exercise of other privacy and data protection rights.
    - Definitions – some definitions had developed over time and would be useful to review, such as consent; pseudonymisation; third party; genetic data; biometric data; health data.
    - A right of the digital person, and neurorights. As processing capabilities develop, consideration should be given to how data protection laws can adapt to address the associated issues with emerging technologies.

3.4 Which other activities do member authorities see as important in achieving high data protection and privacy standards?

Over three-quarters of respondents said that cooperation with regional networks, and with international and multilateral fora, was an activity they undertook to support, promote and implement high data protection and privacy standards. Responses noted that the sharing of knowledge and taking part in joint activities (including joint investigations) plays an important role in the consistent application of high standards, and that international fora can help to establish common and consistent high standards for the protection of personal data, as well as exchanging good practice. It was commented that cooperation of all kinds is needed to support strong privacy development internationally and to support interoperability.

A wide range of networks and fora were mentioned, including the Asia Pacific Privacy Authorities; Asia Pacific Economic Cooperation Data Privacy Subgroup; Association francophone des autorités de protection des données; Council of Europe; European Data Protection Board; Ibero-American Data Protection Network (RIPD); European Conference of Data Protection Authorities (Spring Conference); the GPA; the Global Privacy Enforcement Network; OECD; Common Thread Network; G7 Data Protection and Privacy Authorities Roundtable; Global Cross-Border Privacy Rules Forum (Global CBPR); Berlin Working Group and many other international, regional and federal networks and organisations.

Less than half of the respondents used bilateral agreements for cooperation with other authorities, although comments noted that these can ensure easier solving of issues around complaints received, thus supporting the implementation of high data protection standards and promoting consistency.

Similarly, less than half of the respondents said they were involved in cross-regulatory networks and fora. However, bearing in mind the responses to the earlier question on the importance of cross-regulatory cooperation, this may increase over time.

The majority of respondents consulted with businesses, public authorities and civil society in order to develop, support and promote high standards. It was noted that better understanding industry enabled authorities to understand the practical data protection implications relating to their practices, which in turn enabled them to better guide and regulate those practices. Public and closed consultations on law reform, policies and guidance, surveys, meetings and workshops, and research funding were all mentioned as activities authorities used to develop, support and promote high data protection standards.

3.5 Who is best placed to take forward work to achieve high privacy and data protection standards?

Almost all respondents agreed that supervisory authorities, governments, regional bodies and networks, and international and multilateral fora all had a role to play in taking forward work to achieve high data protection and privacy standards. While governments had a key role in passing data protection and privacy laws, several responses commented that this role was most effective when governments involve supervisory authorities, and consider their views. It was noted that data protection and privacy supervisory authorities have deep, ground-level knowledge which can help to identify and highlight current and emerging issues. Regional and international networks, bodies and fora were noted as being able to play a key role in promoting interoperable frameworks, sharing best practices and endorsing high standards through resolutions or declarations, as well as enabling the establishment of common principles that can be taken into consideration when developing of national regulation.

It was also commented that regional and inter-governmental networks may also be in a position to develop and implement cross-border data transfer mechanisms.

4. Conclusion

The results of the member survey showed a broad level of consensus around the continued importance and relevance of the Madrid principles, many of which are seen as core privacy and data protection principles and rights. It also highlighted the need to recognise that after over a decade of increasing digitalisation and constantly emerging technologies with the ability to process increasing amounts and types of personal data, the strengthening of some provisions, broadening of application, and additional safeguards would be appropriate. Some of these already exist in newer frameworks and instruments such as GDPR and Convention 108+, but all are not yet universally found in all global frameworks and laws.

Almost all respondents supported the idea that the GPA should re-emphasise the Madrid principles in a resolution or policy statement (see section 3.2 above). Noting the survey comments in section 3.5 above, as a body of over 130 data protection and privacy authorities, the GPA is well placed to promote, endorse and advocate for those principles to be incorporated in laws where they are not already, and where they do exist in law, to be effectively implemented and applied to the processing of personal data in new and emerging technologies and innovations as well as more traditional processing. This could be done by way of a resolution or policy statement.

Some of the newer principles, rights and elements not included in the Madrid resolution noted in the survey were agreed by respondents to be important in protecting individuals' privacy and data protection rights and preventing harm. Those with broad agreement could also be included in any resolution or policy statement.

The resolution / policy statement could therefore constitute a call from privacy and data protection authorities for high standards in data protection law and practice in light of increasing digitalisation and emerging technologies and the risks to privacy and data protection they pose. Any adopted GPA position could re-emphasise the importance of applying existing core Madrid principles to these, and advocate for other principles, rights and elements to be adopted by jurisdictions to further develop, implement and support high standards.

Appendix 1 - survey (blank)

GPA Global Frameworks and Standards Working Group

GPA member survey on the GPA's view of high data protection and privacy standards

Introduction

The Global Frameworks and Standards Working Group is mandated by the GPA's Strategic Plan to deliver a resolution or policy statement on the GPA's view of high data protection and privacy standards, for adoption at the GPA 2023. For the next stage of our work we are collecting individual GPA member views on what you see as important in ensuring high data protection and privacy standards. We have developed the survey below – and we'd very much welcome your views.

In our preliminary work over 2021-22, we noted that the GPA last set out its views on high general data protection and privacy standards (as opposed to high standards in relation to particular activities) in 2009, in the Madrid Resolution. Our review of that Resolution found that it appears to be quite comprehensive and forward-thinking for its time, as it includes some important provisions that would still be agreed today as exemplifying high standards – for example key principles are covered, accountability measures included, and the importance of an independent and impartial supervisory authority is emphasised. The resolution also includes a clear expectation that principles and rights should only be restricted by states when necessary and only in certain circumstances, as provided for by national legislation which establishes appropriate guarantees and limits on such restrictions to preserve individuals' rights.

However we recognise that in the 13 years since the Madrid Resolution was adopted, there have been huge and rapid, ongoing changes as the global economy and society has become increasingly digitalised; data protection laws and frameworks have developed and been updated (and with them, new challenges); and regulatory authorities have also evolved. We would therefore like to understand whether today's member authorities of the GPA consider the principles, rights and other elements in the Madrid Resolution still relevant and whether the GPA should re-emphasise their importance, as well as what additional principles, rights and other elements authorities consider as important now – and what will be important to make today's data protection frameworks fit for the future. Your response to this survey will help us build on our review of the Madrid resolution as we consider development of a new GPA resolution or policy statement.

Please complete the survey questions below by the deadline of

25 November 2022

Survey on the GPA's view of high data protection and privacy standards

Authority:	

1. **Do you agree that the principles and other elements in the 2009 Madrid Resolution are still a relevant basis for articulating the GPA's view of high standards? Should they be more strongly emphasised now than they were in the Madrid Resolution?**

   Please complete the table below, answering Yes/No/Not sure for each element, with comments as needed.

Principle / right / element	**Still relevant for high data protection and privacy standards**	**Needs stronger emphasis**	**Comments**
	PART II: Basic Principles		
Lawfulness and fairness	Yes No Not sure	Yes No Not sure	
Purpose specification	Yes No Not sure	Yes No Not sure	
Proportionality	Yes No Not sure	Yes No Not sure	

Data quality	Yes No Not sure	Yes No Not sure	
Openness / transparency	Yes No Not sure	Yes No Not sure	
Accountability	Yes No Not sure	Yes No Not sure	
	PART III: Legitimacy of processing		
General legitimacy of processing (requirement for specific bases for processing)	Yes No Not sure	Yes No Not sure	
Sensitive data (application of extra provisions)	Yes No Not sure	Yes No Not sure	
Provision of processing services	Yes No Not sure	Yes No Not sure	

International transfers provisions	Yes No Not sure	Yes No Not sure	
	PART IV: Rights of the Data Subject		
Access	Yes No Not sure	Yes No Not sure	
Rectification and deletion	Yes No Not sure	Yes No Not sure	
Objection	Yes No Not sure	Yes No Not sure	
Exercise of these rights	Yes No Not sure	Yes No Not sure	
	PART V: Security		
	Yes	Yes	

Security measures	No Not sure	No Not sure	
Duty of confidentiality	Yes No Not sure	Yes No Not sure	
	Part VI: Compliance and Monitoring		
Proactive measures (such as breach prevention procedures; data protection officers; training; audits; privacy by design; privacy impact assessments)	Yes No Not sure	Yes No Not sure	
Monitoring (including provisions for an independent supervisory authority, administrative and judicial remedies to enforce rights)	Yes No Not sure	Yes No Not sure	
Cooperation and coordination (between supervisory authorities, such as sharing investigation techniques and			

regulatory strategies; conducting coordinated investigations; and taking part in working groups and joint fora, and workshops to contribute to the adoption of joint positions, or to improve the technical abilities of authorities' staff)	Yes No Not sure	Yes No Not sure	
Liability (of the data controller / responsible person)	Yes No Not sure	Yes No Not sure	

2. **Does current legislation in your jurisdiction reflect the principles set out in the Madrid Resolution?**

   Yes / No / Not sure

   a. **If No, what are the main differences?**

b. **Is your authority currently calling for changes to the legislation in your jurisdiction, to enhance data protection and privacy standards?**

Yes / No / Not sure

c. **Please comment on what changes your authority is advocating, and/or whether there are any current government proposals to change data protection and privacy legislation in your jurisdiction.**

3. **Should the GPA re-emphasise the principles and other elements from the Madrid Resolution, in the new resolution or policy statement on the GPA's view of high standards, as per your answers to question 1?**

Yes / No / Not sure

Comments:

4. **What additional principles or elements should be included? What additional factors are important as we consider high data protection and privacy standards?**

Principle/right/element	**Should be included as important for high data protection and privacy standards?** **Please rate your answer as follows:** 1. **Strongly support** 2. **Support** 3. **Less strongly support** 4. **Do not support** 5. **Not sure**	**Comments:**
Rights or safeguards relating to automated decisions		
Portability rights		
Right to restriction of processing		

Stronger protections for children and/or vulnerable people		
Stronger emphasis on privacy by design and default		
Access by third-country authorities		
Cross-regulatory cooperation		
Prevention of harms (individual and/or societal)		
Enabling responsible innovation		
Supporting economic growth		
Data ethics		

Other (please add as many as needed)		

6. **What are your current priorities to achieve high data protection standards in your jurisdiction? Are you, and/or others, currently working on this (for example, prioritising for enforcement; developing guidance; advocating legislative change; tracking international developments)? If others are involved, who?**

7. **Do you cooperate with other authorities via networks, forums, MoUs, for example – if so, which, and which do you find most effective in developing and supporting high standards? Why?**

Method of cooperation	**Comments**
Regional networks	

International / multilateral forums	
Bilateral MoUs / agreements	
Cross-regulatory networks and forums	
Other (please add as many as needed)	

8. **Does your authority consult with other stakeholders (such as businesses/other data controllers, and data subjects/the public) about their views on high data protection standards, principles and their practical application? If so, who? Have you published any notable reports or similar on such exercises?**

Stakeholder types	**Yes/No/Not sure**	**Comments and links to relevant reports**
Businesses		
Public authorities		

Civil society		
Individuals		
Others (please add as needed)		

9. **Who is best placed to take forward work to achieve high privacy and data protection standards?**

Body / organisation	**Yes/No/Not sure**	**Comments**
Privacy / data protection authorities	Yes No Not sure	
Governments	Yes No Not sure	
	Yes	

Regional bodies / networks	No Not sure	
International / multilateral bodies / forums	Yes No Not sure	
Other (please add as many as needed)		

Thank you for taking the time to complete the survey. Please submit your response to gpa@ico.org.uk by 25 November 2022

Appendix 2 – survey results - quantitative summary

GFSWG high standards survey quantitative analysis

Principles (Madrid)	**Still relevant**	**Needs stronger emphasis - yes**	**Needs stronger emphasis - no**	**Needs stronger emphasis – not sure**	
Lawfulness and fairness	25	12	7	2	
Purpose specification	26	15	5	1	
Proportionality	25	12	6	2	
Data quality	26	12	6	3	
Openness / transparency	25	17	3	1	
Accountability	25	17	4		
General legitimacy of processing - requirement for specific bases for processing	26	14	5	2	
Sensitive data – extra provisions	26	20		1	
Provision of processing services	22	12	4	5	

International transfers provisions	25	18	2	1	
Rights (Madrid)					
Access	25	13	7	1	
Rectification and deletion	25	12	7	3	
Objection	27	9	6	4	
Exercise of the rights	27	12	6	2	
Security (Madrid)					
Security measures	24	19	4		
Duty of confidentiality	25	6	11	5	
Compliance and monitoring (Madrid)					
Proactive measures	26	18	2	1	
Monitoring	26	16	4		
Cooperation and coordination	25	17	3	3	
Liability	26	14	4	2	
Does current legislation reflect	**Yes**	**No**			

Madrid principles?					
	25	2			
Authority calling for changes to DP / privacy laws?	**Yes**	**No**	**Not sure**		
	12	14	1		
Should the GPA re-emphasise Madrid principles in a new resolution / policy statement?	**Yes**	**No**	**Not sure**		
	26		1		
What additional principles or elements should be included? What additional factors are important as we consider high data protection and privacy standards?					

Additional important principle / right/ element	**Strongly support**	**Support**	**Less strongly support**	**Do not support**	**Not sure**
Rights / safeguards re automated decisions	22	3			1
Portability rights	7	11	3	2	3
Right to restriction of processing	11	12			3
Stronger protection for children and / or vulnerable people	15	8	1		2
Stronger emphasis on privacy by design and default	18	7			1
Access by third-country authorities	12	8	1	1	3
Cross-regulatory cooperation	12	11		1	2
Prevention of harms	10	8	2	1	4

Enabling responsible innovation	6	11	6	3	
Supporting economic growth	4	9	8	2	1
Data ethics	13	7	4	1	1
Others: right to be informed					
Others: definitions – of consent, pseudonymisation, third party.					
Others: include genetic data, biometric data, health data rights of the digital person, and neurorights.[i]					
Current priorities					
Cooperation	**Yes**	**No**			
Regional networks	21				
International / multilateral forums	22				

Bilateral MoUs / agreements	11	3			
Cross-regulatory networks and forums	12	2			
Consultation with other stakeholders	**Yes**	**No**			
Businesses	19	4			
Public authorities	22	4			
Civil society	18	5			
Individuals	16	6			
Others					
Who is best placed to take forward work to achieve high privacy and data protection standards?	**Yes**	**No**	**Not sure**		
Privacy / DPAs	25	1			

Governments	20	2	4		
Regional bodies / networks	20	2	4		
International / multilateral bodies / forums	23	1	2		
Others					Council of Europe Industry

[i] Data items various respondents suggested should be included in sensitive/special data category, and/or that require further safeguards:

Biometric data (10)

Emotional data (1)

Facial recognition (1)

Children (1)

Genetic (7)

Neurodata (1)

Neurorights should be included in DP laws (1)

Criminal convictions and offences (2)

Trade Union membership (1)

Sexual orientation (1)

Health (1)

Political opinion (1)

Data which may be used as a proxy for sensitive data (1)