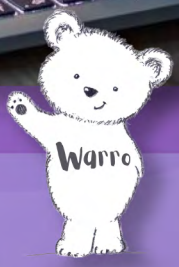
GPA
Global Privacy Assembly

NEWSLETTER

Volume 7 · Issue 2 · Mexico City · May 2024

PAGE 21

The Global Initiative to Elevate Safeguards Against Data Scraping



PAGE 6

Focus

Nigeria´s approach to Data Scraping

PAGE 11

Case Study

Guernsey's approach to Children's Privacy

PAGE 19

Regional Perspectives

Web scraping in Colombia

Index

Message from the Chair

Data Scraping has been one of the main international topics out of the vast ocean of information in Personal Data Protection and Privacy rights. Some members of the Global Privacy Assembly have labored through the International Enforcement Cooperation Working Group in a Joint Statement regarding this interesting theme.

Data Scraping is the automated extraction of data from websites which acts like a net, scooping up information for various purposes. But when this network scoops up personal information, it raises concerns about privacy and the line between public and private in the new technologies.

Members like the Superintendence of Industry and Commerce of Colombia, the Office of the Privacy Commissioner of Canada or the Norwegian Data Protection Authority have underscored the growing awareness of these privacy risks. Publicly available data, the statement argues, can be misused for malicious activities like social engineering scams, identity theft, and bombarding users with spam.

In this edition we present a Latin-American and an African vision of Data Scraping by the Superintendence of Industry and Commerce of Colombia and the Nigeria Data Protection Commission. Our concern is that Data Scraping has become a common practice for various reasons.

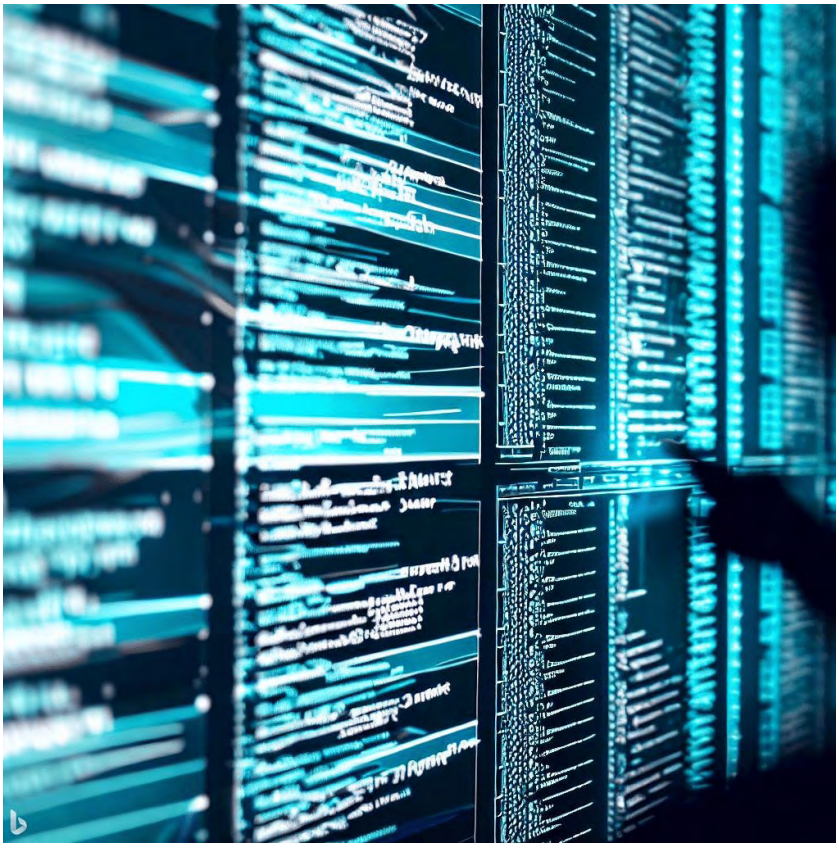
Some of them are that businesses use it for market research, competitor analysis, and price comparison tools. Price aggregator websites, for example, rely on scraping to offer consumers a quick comparison of products across different retailers. Social media platforms themselves sometimes scrape data from public profiles to personalize user experiences, such as suggesting friends or recommending content.

However, the issue becomes more complex when personal information

GPA
Global Privacy Assembly

gets scraped. Names, email addresses, phone numbers, and even location data can be harvested and used for illegitimate purposes.

Just because information is publicly available on a social media profile doesn't necessarily mean the user has consented to its treatment and use by third parties. The joint statement highlights this gap, arguing that scraping personal data can be a privacy violation, even if it's technically accessible to anyone.



On the other hand, this edition also delivers a peek out of the outstanding efforts inside the Global Frameworks and Standards Working Groups lead by the UK Information Commissioner's Office in disclosing the resolution on Achieving global data protection standards: Principles to ensure high levels of data protection worldwide, which includes uprightness of transparency, proportionality, accountability, among another GPA principles.

We have to foreground the GPA's inaugural Privacy and Human Rights Award. "In Conversation With" the Privacy Commissioner of Canada provides us a pronounced perspective when he says that: "is essential to ensure that the privacy protections of individuals are not overshadowed when they are assessed against potentially competing economic interests". There is no doubt that Privacy and Democratic Rights are entwined.

Furthermore, the Horizon Scanning introduces us to the work that the Brazilian National Authority of Data Protection (ANPD) has done over the Regulatory Sandbox for Artificial Intelligence. A great devise that encourage us to regulate new technologies and an inspiration for the rest of Latin American countries to work on similar projects.

Additionally, the Office of the Data Protection Authority of Guernsey gives us a gripping article over Protecting Children's Privacy in the digital age showing us that "a third of children aged 5-7 use social media unsupervised and 24% own a smartphone". We certainly have some work to do over the panorama to promote these privacy rights.

Finally, there is a call for the next GPA meeting that will be held by the Jersey Office of the Information Commissioner. The theme for the 46th Annual Meeting centers around 'The Power of i' and will focus on the core pillars of Information, Individuals, Independence, Integrity, Indigenous, Intercultural, International and Innovation and will explore how these themes interact with harms, values and enrichment of human lives.

As we can see, this edition is enriching, we thank all the authorities who participated, a special mention to The Federal Commissioner for Data Protection and Freedom of Information in Germany (BfDI) for his continuous international support on the GPA's activities. We all together are submerge in the promotion and the defense of the rights to privacy and personal data protection, providing an international vision and validating the commitment to the values of the Global Privacy Assembly. You are now on board this international ship, we invite you to enjoy these avant-garde and enlighten readings.

Nigeria´s approach to Data Scraping

In the dynamic landscape of Nigeria's digital evolution, large-scale data scraping has emerged as a pivotal tool for various industries. From e-commerce giants to government entities, organizations are leveraging scraping techniques to extract valuable insights, enhance competitiveness, and make informed decisions. However, this data-driven journey is not without its challenges, especially concerning privacy and compliance with the Nigeria Data Protection Act (NDP Act) 2023.

Applications Across Industries:

One of the primary sectors benefiting from large-scale data scraping in Nigeria is the e-commerce industry. Companies in the e-commerce sector employ scraping to monitor prices, analyze market trends, and gain a competitive edge. In the financial sector, data scraping plays a key role in uncovering market trends and competitor pricing. Investors can make informed decisions by extracting data from financial forums, news sites, and the stock market.

Challenges:

Challenges such as compliance with data protection regulations, adapting to website structure changes, and performance optimization, require strategic solutions. Hackers employ various techniques, including web scraping, API scraping, AI-powered data scraping to compromise sensitive information. This poses a considerable challenge to organizations aiming to maintain the integrity and security of their data.

Regulatory Landscape:

The NDP Act 2023 establishes the Nigeria Data Protection Commission's (NDPC) ability to issue regulatory instruments to specifically regulate processing of data through various means including Data Scrapping. For instance, Section 6(c) of the NDP Act provides "The Commission shall have powers to issue regulations, rules, directives and guidance under this Act ;"

The National Commissioner/CEO, Nigeria Data Protection Commission (NDPC), Dr. Vincent Olatunji at the Nigeria-Netherlands Economic Consultation. 6th June 2023.

The NDPC organized a Sensitisation Workshop on Data Privacy and Protection for key stakeholders, 20th July 2023

Similarly, under section 24(3), the Act provides thus:

Notwithstanding anything to the contrary in this Act or any other law, a data controller or data processor owes a duty of care, in respect of data processing, and shall demonstrate accountability, in respect of the principles contained in this Act.

In effect, regardless of the purpose of processing and the methodology employed, Nigeria prioritizes the principles of data protection. Where data scrapping for instance is targeted at purposes that require consent under the NDP Act, the consent of the data subjects must be obtained. As a public policy, we are also promoting privacy by design and by default. In this regard, data scrapping which is for statistical purposes may be lawful when the personal data involved is anonymized.

The NDPC is actively engaged in fostering responsible data processing practices. Some of the achievements of the Commission are as follows:

- Capacity building for over 2000 Data Protection Officers to oversee data processing activities of data controllers both in the Public and Private Sectors.
- Sensitization and Strategic awareness engagements with over 80 major data controllers in the public sector
- Active participation as a stakeholder in the formulation of the National Artificial Intelligence policy.
- Encouragement of data controllers and data processors to embrace the culture of privacy by design and privacy by default to mitigate privacy risks.
- Investigation and remediation process for non-conforming organizations.
- Collaboration with regulators to deepen responsible data processing across various sector
- Partnership with other Data Protection Authorities, Networks and development partners for peer review, knowledge exchange and best practices

Balancing Innovation and Privacy:

The Nigerian approach to data scraping reflects a dynamic landscape where innovation and privacy coexist. As organizations leverage scraping techniques for competitive advantage, they must also prioritize compliance with the NDP Act to safeguard individual rights and contribute to the responsible use of data in the digital age.

The (NDPC) organized a workshop for members of ICT & Cybersecurity Committees in the National Assembly on the Implementation of the NDP Act. 7th December 2023.

The Regulation of Artificial Intelligence in Brazil.

By Waldemar Gonçalves Ortunho Junior e Jeferson Dias Barbosa

The development of Artificial Intelligence (AI) in the past years is deeply transforming society, from the way we communicate, to how we interact with the world around us. Considering its potentialities, the risks involved and the global initiatives on the subject, the IA regulation in Brazil is an extremely important issue as it involves aspects that directly impact society, the economy and fundamental ethical principles, such as transparency, justice, fairness and responsibility.

AI has immense potential to drive progress in different areas, such as medicine, education, energy, transportation, among others. However, that entails risks with several impacts on privacy and personal data protection. For this progress to be beneficial to society, it's fundamental to have regulation that stimulates technological advance and promotes its development in a responsible, ethical, and safe manner.

In 2023 it was presented, in the Federal Senate, a legislative proposal[1] that has emerged as a significant milestone in the trajectory of AI regulation in Brazil, with the aim of protecting fundamental rights and guaranteeing the implementation of safe and reliable systems. The proposal reflects the maturity, progress and lessons learned since the start of discussions in 2020 and seeks to establish a balance between the use of technology and the guarantee of fundamental rights of the citizens, without compromising innovation.

About the Brazilian legislative proposition, ANPD has published documents that aimed to analyze it in the light of the data protection legislation.[2] In these documents, the Authority demonstrates its institutional capacity to be the competent authority for regulating AI in Brazil, presenting a proposal of governance with four focus: (i) Advisory Council, with the participation of civil society; (ii) Federal Executive Branch, responsible for formulating and implementing public policies; (iii) Central Authority, with the proposal that ANPD takes on this role; (iv) Regulators' Forum, a committee made up of the central authority and sectoral regulatory bodies with a view to facilitating the coordination and cooperation of their activities.

Attentive to the evolution of discussions around the risks associated with AI systems and concerned about their impact on fundamental rights, ANPD also included the prioritization of the topic of AI in its 2023-2024 Regulatory Agenda at the end of 2022.

One initiative worth highlighting is the development of the Sandbox project, which was put out to public consultation in October 2023[3]. This is an important tool

[1] *Bill No. 2338, of 2023,* which provides for the use of Artificial Intelligence. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233.

[2] NATIONAL DATA PROTECTION AUTHORITY. Preliminary analysis of Bill 2338/2023, which provides for the use of Artificial Intelligence. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-dopl2338_2023-formatado-ascom.pdf. See also: NATIONAL DATA PROTECTION AUTHORITY. ANPD publishes second analysis of the Bill on artificial intelligence. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpdpublica-segunda-analise-do-projeto-de-lei-sobre-inteligencia-artificial

that aims to support possible regulation on the subject and foster responsible innovation in AI. ANPD's Sandbox could provide elements for testing innovative products, services and approaches within a limited sector or domain, to assess the regulatory impact and outcome. This approach balances regulation through experimentation, ensuring that appropriate safeguards are in place.

ANPD plans to include machine learning-driven technologies, including those related to generative AI, in the scope of the project. It is worth mentioning that in January 2024, the Sandbox project led by ANPD was cited in the Artificial Intelligence Governance Report published by the World Economic Forum[4].

ANPD is very active in the discussion about AI regulation in Brazil, not only due to its competence to ensure data protection, but also because of its primary commitment to the fundamental rights of citizens, as holders of personal data. In this sense, the Authority, with its structure, knowledge and technical capacity, is ideally suited to play a leading role in regulating AI in Brazil.

[3] *NATIONAL DATA PROTECTION AUTHORITY.* Open consultation on the regulatory sandbox for artificial intelligence and personal data protection in Brazil. Available at: https://www.gov.br/anpd/ptbr/assuntos/noticias/abertaconsulta-a-sociedade-sobre-sandbox-regulatorio-de-inteligencia-artificial-e-protecao-dedados-pessoais-no-brasil.

[4] WORLD ECONOMIC FORUM. Generative AI Governance: Shaping a Collective Global Future. Available at: https://www3.weforum.org/docs/WEF_Generative_AI_Governance_2024.pdf.

Cristo Redentor, Rio de Janeiro, Brazil. Photo by Athena Sandrini

Horizon Scanning

A Regulação da Inteligência Artificial no Brasil

By Waldemar Gonçalves Ortunho Junior e Jeferson Dias Barbosa

O desenvolvimento da Inteligência Artificial (IA) nos últimos anos vem transformando profundamente a sociedade, desde a forma como nos comunicamos até mesmo como interagimos com o mundo ao nosso redor. Considerando as suas potencialidades, os riscos envolvidos e as inciativas globais sobre o tema, a regulação da IA no Brasil é um tema de extrema importância, na medida que envolve aspectos que impactam diretamente a sociedade, a economia e princípios éticos fundamentais, como transparência, justiça, equidade e responsabilidade.

A IA possui um potencial imenso para impulsionar o progresso em diversas áreas, como a medicina, educação, energia, transportes, entre outras, porém implica em riscos com impactos significativos à privacidade e à proteção de dados pessoais. Para que esse avanço seja benéfico para a sociedade, é fundamental que haja uma regulamentação que estimule o avanço tecnológico e proporcione o seu desenvolvimento de forma responsável, ética e segura.

Em 2023 foi apresentado no Senado Federal uma proposta legislativa[1] que surgiu como um marco significativo na trajetória de regulação da IA no Brasil, com o objetivo de proteger direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis. A proposta reflete o amadurecimento, os avanços e os aprendizados acumulados desde as discussões iniciadas em 2020 e busca estabelecer um equilíbrio entre

o uso da tecnologia e a garantia dos direitos fundamentais dos cidadãos, sem comprometer a inovação.

Em relação à proposição legislativa brasileira, a ANPD produziu documentos que buscaram analisá-lo à luz da legislação de proteção de dados, os quais foram divulgados em seu sítio eletrônico[2]. Nestes documentos a Autoridade demonstra a sua capacidade institucional para ser a autoridade competente na regulação da Inteligência Artificial no Brasil, apresentando proposta de governança com quatro eixos de atuação: (i) Conselho Consultivo, com participação da sociedade civil; (ii) Poder Executivo Federal, responsável pelas atribuições de formular e implementar políticas públicas; (iii) Autoridade Central, com a proposta de que a ANPD assuma esta função; (iv) Fórum de Reguladores, comitê integrado pela autoridade central e por órgãos reguladores setoriais com vistas à facilitar a coordenação e a cooperação de suas atividades.

Atenta à evolução das discussões em torno dos riscos associados aos sistemas de IA e preocupada com o seu impacto nos direitos fundamentais, a ANPD incluiu, já no final do ano de 2022, a priorização do tema de IA na sua Agenda Regulatória 2023-2024.

Uma iniciativa que merece destaque

é o desenvolvimento do projeto de Sandbox, colocado em consulta pública em outubro de 2023[3]. Esta é uma importante ferramenta que visa subsidiar eventual regulação sobre a temática e fomentar a inovação responsável em IA. O Sandbox da ANPD poderá fornecer elementos para o teste de produtos, serviços e abordagens inovadoras dentro de um setor ou domínio limitado, para avaliação do impacto e o resultado regulatório. Essa abordagem equilibra a regulamentação por meio da experimentação, garantindo que salvaguardas adequadas sejam aplicadas. A ANPD planeja incluir no escopo do projeto tecnologias impulsionadas por aprendizado de máquina, incluindo aquelas relacionadas à IA generativa.

Vale mencionar que, em janeiro de 2024, o projeto de Sandbox conduzido pela ANPD foi citado no Relatório de Governança de Inteligência Artificial, publicado pelo Fórum Econômico Mundial[4].

Portanto, a ANPD está bastante ativa na discussão a respeito da regulação da IA no Brasil, não apenas pela sua competência de zelar pela proteção de dados, mas também pelo seu compromisso precípuo com os direitos fundamentais dos cidadãos, na condição de titulares de dados pessoais. Nesse sentido, verifica-se que a Autoridade com sua estrutura, conhecimento e capacidade técnica, está idealmente vocacionada para desempenhar um papel de liderança na regulação da IA no Brasil.

[1] • *Projeto de Lei nº 2338, de 2023, que dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233.*

• AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analisepreliminar-do-pl-2338_2023-formatado-ascom.pdf.

[2] *AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD publica segunda análise do Projeto de Lei sobre inteligência artificial. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-segundaanalise-do-projeto-de-lei-sobre-inteligencia-artificial.*

[3] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Aberta consulta à sociedade sobre sandbox regulatório de inteligência artificial e proteção de dados pessoais no Brasil. Disponível em: https://www.gov.br/anpd/ptbr/assuntos/noticias/aberta-consulta-a-sociedade-sobre-sandbox-regulatorio-de-inteligencia-artificial-e-protecao-dedados-pessoais-no-brasil.

[4] WORLD ECONOMIC FORUM. Generative AI Governance: Shaping a Collective Global Future. Disponível em: https://www3.weforum.org/docs/WEF_Generative_AI_Governance_2024.pdf.

Guernsey's approach to Children's Privacy

By Brent R Homan, Data Protection Commissioner Guernsey

As Nelson Mandela said, "there can be no keener revelation of a society's soul than the way in which it treats its children."

At the Office of the Data Protection Authority in Guernsey ("ODPA"), protecting and promoting the rights of children is at the heart of our strategic plan and explicitly written into our data protection laws. And that is not surprising. In fact, it is a reflection of the deep commitment that Guernsey residents have towards the care of their most cherished treasure – our children.

You have heard the expression, "it takes a village to raise a child", well in Guernsey we recognize that "it takes an island to protect our children" which is why our strategy demands contributions and action from every key stakeholder – regulator, educators, parents, business leaders, and most importantly – the children themselves.

To this end, the ODPA's dedicated youth outreach programme, 'Project Bijou Seeds', which is led by a qualified teacher, educates hundreds of children every year via in-school sessions about how to navigate the online world safely. To complement these conversations and target the younger kids, the ODPA has written a children's book about an inquisitive bear named Warro who goes on an adventure in the digital world while wondering "Who is asking for my information, what do they want to know, why do they want it, where will it go?"

Whether in schools or in the pages of a children's book, delivering a balanced message is key. Protecting children is certainly not about banning them from the online and virtual world. Any parent knows how well that conversation goes! And there are so many benefits to engaging and connecting in the digital era, as long as we navigate the online landscape with care.

But as far as risk goes, our collective vigilance has never been more in demand. A recent report by UK communications regulator Ofcom found that a third of children aged 5-7 use social media unsupervised and 24% own a smartphone. In fact, only a third of parents know the correct minimum age requirement for most social media platforms.

And this is why empowering parents has also been a key pillar of our strategy. Back in January of this year the ODPA issued a Bailiwick Data Protection Advisory alerting residents of a local Snapchat group where children were encouraged to

share indecent images of themselves.

In that advisory and subsequent BBC TV and radio interviews, we called upon parents to actively engage with their children and have conversations about the reputational and long-term risks associated with sharing personal information (including photos) via such networks, that could then find an indelible presence online. Parents were also reminded of their responsibility to exercise parental oversight and controls to ensure that their children are not on networks and apps for which they are not of an authorized age.

The genuine and immediate outpouring of concern amongst Guernsey's parents and educators to these events was staggering, leading to a 'Roundtable on protecting children online' where Bailiwick education leaders shared experiences, challenges and strategies towards elevating the protection of children and their information in today's digital era.

So how do we leverage the wealth of collective stakeholder knowledge, experience, strategies and energy toward maximizing the protections afforded to our children?

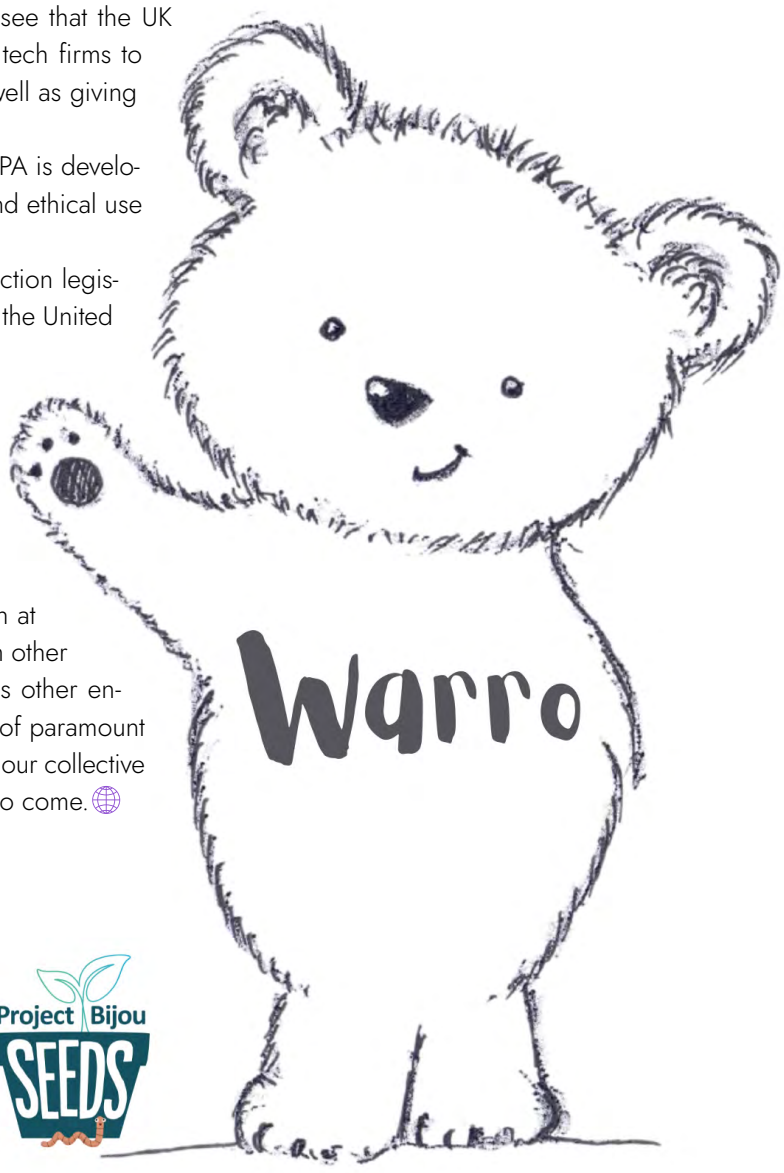
If we look at legislative actions beyond our shores we see that the UK Online Safety Bill became law last year and aims to force tech firms to take more responsibility for content on their platforms, as well as giving regulator Ofcom more enforcement powers.

In the absence of similar legislation in Guernsey, the ODPA is developing a 'Children's Framework' to support the responsible and ethical use of information about children.

It will combine the legal requirements of local data protection legislation with the relevant principles and provisions outlined in the United Nations Convention on the Rights of the Child.

The framework itself should lead to clear, relevant and practical guidance on how best to look after young people's data. It will encourage a child-centric approach that normalises high standards of governance for anyone handling personal data involving children.

Finally, it is evident that we are not alone amongst regulatory counterparts in placing the protection of our children at the highest level of priority. Which is why collaboration with other agencies both within the data protection realm, and across other enforcement and regulatory spheres such as online safety, is of paramount importance. By speaking with a unified voice we can expand our collective capacity to protect our children today and for generations to come.



THE OFFICE OF THE Data Protection Authority

Project Bijou SEEDS

Resolutions with lasting impact

Achieving Global DP Standards

Photo by AXP Photography

By Chris Taylor, Director Regulatory Strategy – International, UK Information Commissioner's Office and Chair of the GPA Global Frameworks and Standards Working Group

They say time flies. We're now over halfway through the GPA year and many of us will already be looking forward to the GPA2024. But it is also a good time to look at how we're ensuring the resolutions we adopted in 2023 continue to have impact, influencing global data protection policy and encouraging high standards worldwide.

The UK Information Commissioner's Office (ICO) was the main sponsor of two resolutions at the GPA 2023. The first was the resolution on Achieving global data protection standards: Principles to ensure high levels of data protection worldwide, which we led as chair of the Global Frameworks and Standards Working Group (GFSWG).

The resolution highlights a set of common principles, rights and other key practical elements - high-level data protection standards that we will promote worldwide, to increase protections for people and certainty for organisations wherever data flows – while recognising that all laws don't have to be identical.

It includes principles such as transparency, proportionality, accountability, enforceable rights and highlights the importance of protections for children, and privacy by design and default. The principles are mostly familiar and already appear in many laws globally – but not all. The resolution shows that these principles stand the test of time and can (and should) be applied in the current and future contexts. See these FAQs for further information.

The resolution provides a reference point for GPA members and others to use in their own domestic jurisdictions, to influence governments and other stakeholders as laws are developed and reviewed. The ICO has shared it with the UK government, and we know some other GPA members have already done the same in their countries.

It can also be used to influence internationally – for example via the UN, OECD, Council of Europe and regional and linguistic networks in their work – to increase protection for people globally. The resolution has already been presented to several organisations by various GFSWG members and we're delighted to see that it has been referenced in a report and speech by the UN Special Rapporteur on the Right to Privacy.

Additionally, by highlighting common approaches that GPA members have to core principles and rights, the resolution can support discussions around convergence and interoperability of frameworks and cross border transfer mechanisms.

Greater London, England, United Kingdom. Photo by John Smith

The second ICO-led resolution (together with our Italian and German colleagues) is a good example of how we should apply these high-level principles to a particular issue that challenges us all – AI. The Resolution on Artificial Intelligence and Employment highlights that the data protection and privacy risks associated with AI in the employment context can cause serious harm - changing livelihoods, significantly impacting career prospects and resulting in discrimination.

Building on the GPA's previous substantial work on AI, it sets out how to address those risks during the development and deployment of AI in the employment context. It emphasises principles of explainability, data quality and security, the importance of data protection impact assessments, and careful consideration of the sources of data used to train AI models. It highlights the importance of human review of automated decisions, and the ability of people to obtain redress if things go wrong. It also addresses higher risk uses of AI to infer emotions, which should not be used except in limited circumstances subject to robust testing.

The ICO has been promoting these provisions at conferences and in bilateral meetings with stakeholders, and we know our co-sponsors have done so in discussions with their governments, in their guidance and casework.

We have a positive story to tell so far, but it's not finished yet. Continued GPA member collaboration to promote consistent approaches is crucial to ensure we maximise the impact of our resolutions, influencing global data protection policy to provide better protection for people worldwide and more regulatory certainty for organisations - not just this year but also in the future.

Recognizing privacy in support of other fundamental rights

Launching the GPA's inaugural Privacy and Human Rights Award

By Philippe Dufresne, Privacy Commissioner of Canada

This year, almost half of the world's population will be participating in national elections. In this context, it is timely for us as members of the Global Privacy Alliance (GPA) to highlight the role that privacy plays in protecting and upholding democratic processes.

The recognition and protection of privacy as a fundamental right underscores the importance of the GPA's Data Protection and Other Rights and Freedom (DPORF) Working Group. I share this commitment and it is an honour for me to Chair the DPORF Working Group and further the acknowledgement that privacy is not just a fundamental right, but that it critically underpins the protection and recognition of all other human rights.

As the GPA noted in the 2019 resolution on privacy as a human right, privacy is a precondition for citizens' other freedoms as well as a keystone right for democracy.

Office of the Privacy Commissioner of Canada

As Privacy Commissioner of Canada, I am continuing to advance the work of the GPA DPORF Working Group both in Canada, as well as internationally. In Canada, I have been championing the recognition of privacy as a fundamental right in our existing federal privacy legislation, the Personal Information Protection and Electronic Documents Act and the Privacy Act. This is essential to ensure that the privacy protections of individuals are not overshadowed when they are assessed against potentially competing economic interests.

This past December, as DPORF Chair and with the support the Working Group, I issued a joint statement with the United Nations Special Rapporteur on the Right to Privacy, Dr. Ana Brian Nougrères, on Privacy and Democratic Rights. This statement showcases the role that privacy and data protection play in upholding democratic rights and freedoms, and why this must be so strongly protected.

When I was appointed as Canada's Privacy Commissioner almost two years ago, in June 2022, the first pillar of my vision for privacy, consistent with the work of the GPA, was that privacy is a fundamental right. This pillar has continued to underpin my work as Commissioner, driving my Office's new three-year strategic plan, as well as my broader

Parliament Hill. Ottawaw, ON, Canada. Photo by Tetyana Kovyrina

engagement in the global privacy community.

The right to privacy underpins the personal flourishing and development of individuals as citizens, as well as their ability to exercise social and political freedoms and to participate in democratic processes. Privacy is a key protection from undue influence and manipulation of individuals and is important to protect open, equitable democratic processes.

Data protection authorities play a critical role alongside others, including legislators, political parties, digital platforms and other regulators, to work together to support the protection of these interconnected rights.

The DPORF Working Group provides a key contribution to the GPA Strategic Plan. Building on the resolution that was adopted at the 45th GPA in Bermuda last October, the Working Group is preparing to launch the GPA's inaugural Privacy and Human Rights Award to help elevate the GPA's influence as a global leader in privacy and data protection by recognizing the work that others in the broader privacy community are doing to further this cause.

With deep appreciation for the efforts of our colleagues on the Working Group, I am pleased to share that the GPA's inaugural Privacy and Human Rights Award will be officially launched in June, with the nomination period open through the end of August.

The Award will celebrate exemplary work by an organization to promote and protect privacy and other fundamental rights. Courtesy of Access Now, the selected award recipient will attend the 2025 RightsCon Conference, where they will be officially recognized in front of a global audience of privacy and human rights advocates and celebrated for their achievements.

I believe that this award is a positive step towards advancing the GPA's mission of recognizing and elevating privacy discourse and I look forward to the opportunity to celebrate the work of other organizations to champion privacy and other fundamental rights.

Global participation in this award process is important to share the news widely and reach those who are most deserving of recognition. I look forward to your support in promoting this award and to seeing the nominations of the incredible work that is being done to champion privacy and other fundamental rights around the world.

Protecting privacy is one of the paramount challenges of our time. Like all of you, I am committed to doing my part, through strong advocacy, education, promotion, and enforcement. This is a collective effort that relies on many voices, and a wide spectrum of representation, to ensure that our message and themes remain as universal as possible.

I thank you for your support and continued work to protect and uphold privacy as a fundamental right around the world.

Get to know your ExCo:

The Federal Commission for Data Protection and Freedom of Information of Germany (BfDI)

By Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information in Germany

Reichstag building, Berlin, Germany. Photo by Niki Nagy.

In our digital age, where data are transferred across borders on a global scale, the protection of personal data, effective enforcement of the law by supervisory authorities and enforcement cooperation become ever more important.

Since I took the office of Federal Commissioner for Data Protection and Freedom of Information (BfDI) in Germany in January 2019, I have considered international collaboration as one of my top priorities. I therefore highly value my involvement in the Global Privacy Assembly (GPA) and its Executive Committee, where I have been an elected member since October 2020. The GPA plays an important role in fostering cross-border cooperation and promoting high international standards in data protection and privacy.

My international engagement in the GPA - as well as in other international fora and organizations such as the G7 Roundtable of Data Protection and Privacy Authorities, the Council of Europe, the OECD or the International Working Group on Data Protection in Technology (IWGDPT, "Berlin Group") - is directed towards supporting international collaboration and upholding the fundamental right to data protection and privacy in an international context to the highest extent possible.

The office of the Federal Commissioner for Data Protection and Freedom of Information (BfDI) was established in 1978 under the Federal Data Protection Act (BDSG). Headed by the Federal Commissioner, who is elected by the Federal Parliament ("Bundestag"), the BfDI operates independently to ensure impartiality and effectiveness in its regulatory functions. Currently, the BfDI office consists of four directorates with 30 units and more than three hundred staff members.

Over the past few years, my office has been entrusted with new tasks in the public as well as in the private sector, including capacity building in technology. This has led to a growing number of employees in order to cover these new tasks and challenges. Responsibilities of my office include policy advocacy, advising government bodies, handling and investigating complaints of individuals and, in particular, monitoring compliance with data protection laws by federal authorities and by actors within specific

economic sectors (Telecommunication, Postal Service Providers) in Germany. Due to the federal system in Germany, I share responsibilities with the Supervisory Authorities of our Federal States, the "Länder", which are competent for data protection in remaining areas of the public and the private sector.

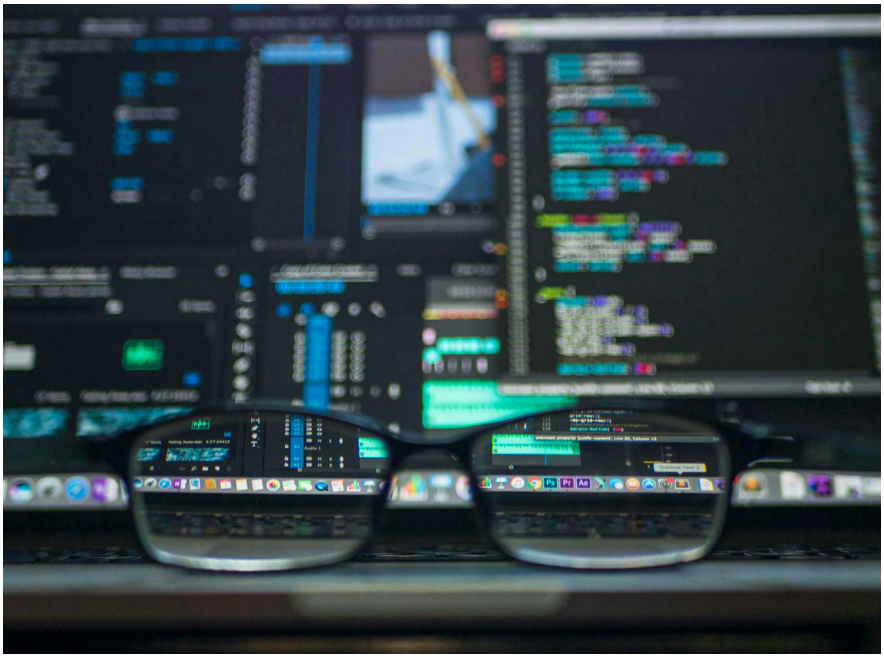
Given this plurality of German Supervisory Authorities, one of my key obligations is to act as the Joint Representative of the German Data Supervisory Authorities in the European Data Protection Board (EDPB), where I coordinate the German positions and contributions to the EDPB´s work.

At the heart of the GPA is its Executive Committee, comprising elected representatives from member authorities as well as current, future and previous hosts of the GPA Annual Meetings. The Executive Committee therefore reflects the diversity of the GPA's more than 130 member organizations and ensures its inclusive approach by taking into account relevant regional and jurisdictional perspectives.

The Executive Committee plays a decisive role in guiding the direction of the GPA's work according to its multi-annual Policy Strategy, and in representing its members' interests on the global stage. I feel honored and privileged to contribute to this work since 2020, for example as the first chairperson of the GPA Reference Panel after its establishment in April 2021, or as a member of the "Strategic Direction Sub-Committee" (SDSC). In addition to this, my international team is active in the "Host Bid Selection Sub-Committee" of the Executive Committee as well as in several GPA Working Groups.

With regard to the future, I am convinced that the GPA, its Executive Committee and its Working Groups will continue to be crucial for upholding and promoting data protection and privacy rights in in the evolving digital landscape.

Web scraping in Colombia



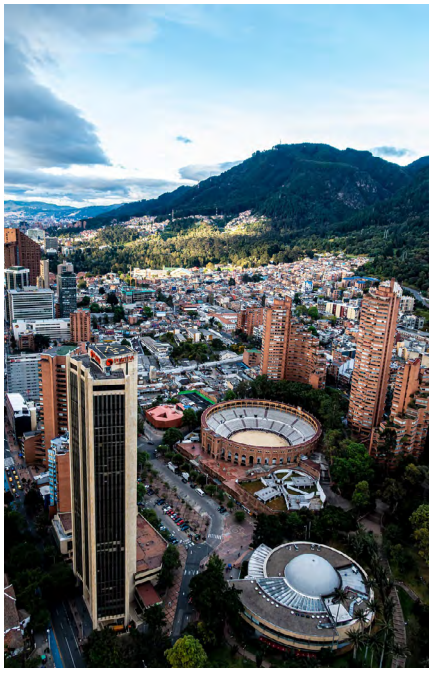
By Grenfieth De Jesus Sierra Cadena, Superintendente de Industria y Comercio de Colombia

Web scraping has emerged as a practice that poses first-level legal and technical challenges for the protection of personal identity in the online world. Illegal activities that threaten the dignity of individuals are taking place.

Identity theft is a practice that can end up causing deep harm to a human being and their environment, especially when personal data can be manipulated using artificial intelligence. The line between reality and the simulation of a person can be porous and difficult to mark. If what a person is can be confused with fiction and the simulation that an AI-powered software can produce, then we are facing a challenge that should alert all international data protection authorities. This calls for dialogue, coordination, and harmonization of solutions.

This practice can occur for both commercial and criminal activities. In both cases, it is necessary to impose limits and exercise sanctions. Both the company that does not implement adequate protection of the personal data it processes and whoever clandestinely decides to extract and exploit them without proper consent must be subject to legal sanctions. The former bears responsibility for not exercising the Principle of Accountability, which calls for proper administration and protection of legally collected data. They have failed in the framework of protection that their role as an administrator imposes on them. The latter is responsible for an illegal and criminal practice aimed at exploiting and manipulating personal data to distort reality by impersonating the data subject or creating new identities without legal support in the real world. Sanctions in such cases must be administrative, but with a greater emphasis on punitive criminal consequences. The level of risk is very high for the data subject, and the violation of rights is structural. Those who engage in this practice are aware of its illicit nature.

Regarding data administrators, it is necessary to differentiate between public and private actors. Private entities are governed by contractual information clauses to the data subject and the duty of protection they have over collected data. However, public administrators



Bogota, Colombia. Photo by Germán Rojas.

Bogota, Colombia. Photo by Mario Alejandro González

seem to assume lower levels of responsibility considering the principle of transparency of information. Therefore, authorities must verify and implement necessary security and transparency measures to inform that while a piece of information may be publicly accessible, this does not mean it is public data for indiscriminate use. For example, the information of public servants in Colombia, which is public accessible for purposes of control and transparency but is personal and intended for restricted use due to purpose limitation.

The SIC in Colombia, through Resolution 58834 of 2023, has highlighted these differences in one case, calling for better practices of information, security, surveillance, monitoring, and sanctions for both public and private data administrators as means of protection and prevention against web scraping.

As the Colombian DPA, we find it necessary to propose solutions and ways to sanction those who engage in this practice without the consent of data subjects. The other method must be criminal and must guarantee investigations and sanctions against cybercrime networks worldwide. International coordination of data protection authorities is essential in both administrative and criminal spheres. It is a global challenge, and the response must be global.

Joint data scraping initiative leverages collaboration to improve privacy and data protection

By **Michael Maguire**, *Director of PIPEDA Compliance, Office of the Privacy Commissioner of Canada (IEWG Co-Chair)*

The Joint statement on data scraping and the protection of privacy is the latest in a series of impactful collaborative compliance initiatives of the Global Privacy Assembly's (GPA) International Enforcement Cooperation Working Group (IEWG), demonstrating that by working together, privacy enforcement authorities can expand capacity and amplify the impact on protection of privacy and personal data.

Unlawful data scraping can result in a wide array of privacy risks to affected individuals, ranging from the receipt of unwanted marketing messages, to identity theft and fraud, and unauthorized mass surveillance and cyber-attacks. It is integral to the global digital economy and society that individuals feel confident and safe engaging online, without fear that their personal information will be used in ways that they hadn't intended and that may cause them harm. In the face of such risks and following reports of numerous incidents of mass data scraping affecting millions of individuals worldwide, the IEWG undertook an initiative to foster better protection of the vast amount of personal data accessible online.

The IEWG, which became a permanent working group of the GPA in 2018, regularly holds "closed enforcement sessions" wherein member authorities come together to converse about emerging privacy issues of global importance and interest, and where appropriate, to agree on collaborative initiatives to enhance global privacy and data protection. The Joint statement, which has been endorsed by 14 privacy enforcement authorities from six continents[1], was a direct outcome of two such meetings, initiated by Australia (OAIC) and Hong Kong (PCPD).

A subgroup of the IEWG, co-led by Canada (OPC) and Australia (OAIC), drafted and published the joint statement in August 2023, highlighting several key messages:

- Publicly accessible personal data is subject to data protection laws in most jurisdictions.
- Social media companies and the operators of websites that host publicly accessible personal data have obligations to protect that information from unlawful data scraping (the statement also suggested a non-exhaustive list of potential safeguards).
- Mass data scraping incidents can constitute reportable data breaches in many jurisdictions.
- Individuals can also take steps to protect their personal information from data scraping.

[1] The joint statement was initially signed by the privacy enforcement authorities of Australia, Canada, United Kingdom, Hong Kong, Switzerland, Norway, New Zealand, Colombia, Jersey, Morocco, Argentina and Mexico, and subsequently endorsed by Guernsey and Spain.

Alexandra Bridge, Ottawa, Canada. Photo by Gabriel Macías.

The co-signatories shared the joint statement with six of the world's largest social media companies, seeking their feedback. This resulted in a fruitful dialogue with a number of those companies, as well as other key industry players. This allowed the working group to expand its understanding of data scraping, including in relation to new and innovative privacy-protective practices to counter ever-evolving data scraping threats, the use of AI against data scraping and the use of data scraping to feed AI, and mechanisms for granting controlled access to publicly accessible personal data for potentially socially beneficial purposes.

This initiative has and will continue to raise awareness of the important issue of data scraping, including through panel engagements at global privacy events such as the IAPP Global Summit and the upcoming Venice Privacy Symposium. It has also allowed co-signatories to amplify their common message that companies must implement appropriate measures to protect the personal data that they collect and make publicly accessible on their platforms and has demonstrated the value of informal compliance actions and proactive engagement with industry towards improving global privacy protection.

The IEWG data scraping sub-group looks forward to sharing further takeaways in a final statement to be issued in advance of the upcoming GPA Conference.

Have you secured your tickets for the **46th Global Privacy Assembly in Jersey, Channel Islands?**

Jersey Office of the Information Commissioner honoured to be hosting annual conference for 2024

Jersey Information Commissioner Paul Vane and his Jersey Office of the Information Commissioner (JOIC) team are honoured to be hosting the 46th Global Privacy Assembly and invite you to join them for our annual conference in the beautiful Island of Jersey, Channel Islands, from Monday 28 October 2024 to Friday 1 November 2024.

46th Global Privacy Assembly Theme 'The Power of i'

The theme for the 46th annual conference centres around 'The Power of i' and will focus on eight core pillars of Information, Individuals, Independence, Integrity, Indigenous, Intercultural, International and Innovation. Discussions will highlight the significance of the eight themes, which are intrinsically linked to encompass the harms, values, and enrichment of our human lives. The discussions will challenge and question who controls this power, for what purpose, and for whom. They will also examine the effectiveness of current regulatory models, questioning whether they are still fit for purpose in a rapidly changing world. The conference aims to create a roadmap for the future, both short- term and long-term, to improve individuals' ability to self-manage their data, achieve greater equity in data sharing, and foster better behaviours and culture around the use of personal data.

BUY TICKETS, WATCH
LAUNCH VIDEO AND FIND OUT MORE AT

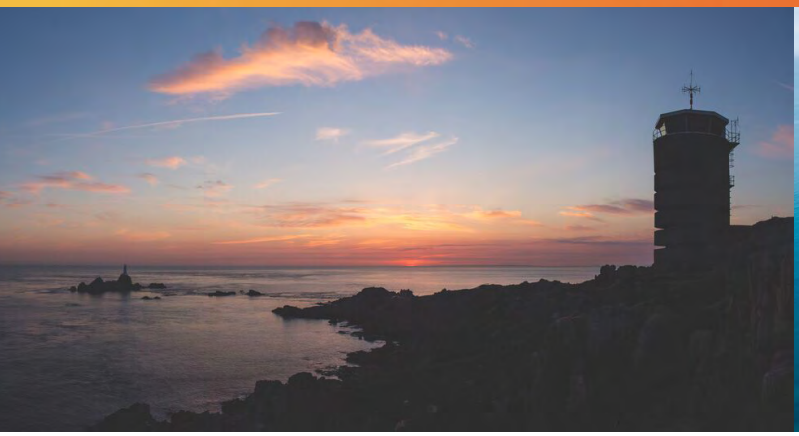
www.gpajersey.com

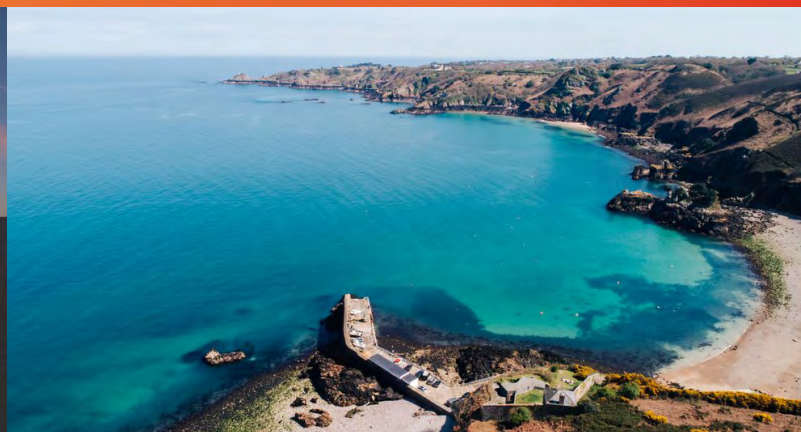
Conference Schedule and Agenda

The 46th conference schedule will include a Welcome Reception on Monday 28 October 2024, hosted in Jersey's capital and largest district, St Helier. This will lead into two consecutive days of Open Conference Sessions held at the prestigious Royal Jersey Showground in the district of Trinity. These will be concluded by a Gala Dinner and Awards Night and lead into a day and a half of Closed Conference Sessions held at the Radisson Blu Hotel overlooking the St Helier marina.

The Open Session agenda will explore the future of privacy regulation, asking how Data Protection Authorities will need to adapt over the next 30 years, how technology will impact regulators and what does our future as digital regulators look like. The agenda will highlight the Individual, asking 'Who Cares About One Person?' and discussing how elevating the individual elevates all humanity. Other keynotes will question the role of data privacy in environmental initiatives and humanitarian crisis.

Catwalk debates, panel discussions, parallel sessions and fireside chats will discuss how we reduce inequalities in privacy rights to protect our most vulnerable citizens, Regulatory Cousins and how regulators tackle the challenge of overlapping policy domains, as well as the importance of hearing the voices of the next generation, the societal impact of privacy education and how indigenous communities develop their own data protection frameworks.





About Destination Jersey

Travel and Accommodation Information

An Island shaped by the sea, Jersey is the largest of the British Channel Islands, at 45 square miles in size. 100 miles from the south coast of England and 14 miles from the coast of France, Jersey combines British charm with continental flair. Delegates can enjoy breathtaking landscapes, rich heritage and a unique island atmosphere. It is not a city break, country break or beach break, Jersey is all these things and more, making the Island an ideal conference destination.

With over 20 departure points from the United Kingdom and Ireland, getting to Jersey is easy. You can fly from London to Jersey in just 40 minutes. The JOIC conference team has connections with a range of Jersey hotels and preferable accommodation rates are available based on bookings for a four-night period from Monday 28 October to Friday 1st November 2024. These are being sold on a first come, first served basis and block booking holds and preferential rates are secured until Friday 4 August 2024. Additional nights can be booked by contacting the hotels directly.

Registration for the 46th Global Privacy Assembly is open now. To watch the conference launch video, find out more about Travel, Accommodation, Jersey as a destination and Register, visit the JOIC's dedicated conference website www.gpajersey.com.

For conference updates connect with the Jersey Office of the Information Commissioner on Facebook, LinkedIn, X and Instagram and search #GPAJSY2024. Commissioner Vane and his team ask you to please share the 46th conference content across your organisation and individual, professional, social media profiles, to raise awareness of the event.

BUY TICKETS, WATCH LAUNCH VIDEO AND FIND OUT MORE AT

www.gpajersey.com

For more information please contact the JOIC Communications Team at communications@jerseyoic.org or via the JOIC main line +44(0)1534 716530.

JerseyOIC jersey_oic jerseyOic Jersey Office of the Information Commissioner

GPA

Global Privacy Assembly