IAPP Europe Data Protection Congress 2022
Schedule & Programme

Tuesday, 15 November

9:00 – 13:00

[Tuesday, 15 November, 9:00 – 13:00]
AI for Privacy Professionals

Jose Belo, CIPP/E, CIPM, FIP, Head of Data Privacy, Valuer.ai
Christian Lawaetz, Chief Technology Officer, Co-Founder, Valuer.ai
Lucia Canga Roza, CIPP/E, Legal Counsel, Data Protection, Toyota Motor Europe

The many companies using artificial intelligence systems all face the same need to ensure their models operate in a legally compliant, ethical and transparent way. Determining whether a model is operating in a "reasonable" manner regarding biased outputs and impacts, while protecting personal data, is a must. The challenges around doing so are legion. In this workshop, you will learn strategies to evaluate production-level AI for bias and fairness, particularly as it applies to protected classes. We will go beyond 101-level discussions of training data to discuss how construction of machine learning features and internal research and analysis impacts bias and privacy concerns. Likewise, we will discuss how some priorities for making AI ethical may create accuracy and privacy challenges of their own.

What you will learn:
• An overview of production versus research AI and machine learning.
• A review of privacy risks in productionised AI.
• Risks and remedies for privacy in proposed AI regulations.

Additional registration fee required.

(Tags: Workshop, Ethics, Policy & Governance, Privacy Operations Management)

[Tuesday, 15 November, 9:00 – 13:00]
Data Transfers Master Class

Victoria Hordern, CIPP/E, CIPT, Partner, Taylor Wessing
Richard Montbeyre, CIPM, CPO, DPO, BMC Software
Olivier Proust, CIPP/E, Partner, Privacy, Security and Information, Fieldfisher

The so-called "Schrems II ruling" by the EU Court of Justice sent a shockwave through the world of privacy by invalidating the EU – U.S. Privacy Shield. But more importantly, it has paved the way for a new set of rules and requirements that require organisations to assess their data flows, review the laws in third countries and determine whether they must implement any "supplemental measures" that will allow them to continue to transfer personal data outside the EU. From an organisational standpoint, organisations are struggling to understand how they can continue to transfer personal data outside the EU, including to the U.S. During this masterclass, we will discuss the key developments that have marked 2021 and 2022, including TIA, SCC, Privacy Shield 3.0, BCR and Brexit.
What you will learn:
• A deeper understanding of the GDPR's rules on transfers of personal data outside the EU.
• The latest information on legislative and regulatory developments that affect data transfers.
• Experiences, best practices and tips from legal practitioners regarding the transfers of personal data outside the EU.

Additional registration fee required.

(Tags: Workshop, Policy & Governance; Privacy Law; Trans-Border Data Flow; European Union)

[Tuesday, 15 November, 9:00 – 13:00]
Harnessing the Power of Metrics: Measuring and Reporting for Programme Success

Simone Fennell, CIPP/E, CIPM, FIP, Privacy Advisor, City of Tilburg; Trainer, Privacy Company
Martin Zinke, CIPP/E, CIPM, Senior Consultant, Verdonck Klooster & Associates

What gets measured gets done. But how do you go about developing and maintaining a privacy metrics programme that both measures where you are today and helps you meet your objectives for tomorrow? KRIs and KPIs can be used across an organisation to measure how risky certain activities may be and how well you are managing those risks. Applying privacy metrics like KRIs and KPIs to a privacy programme can be an additional source of information around how individuals view your data handling practices. Learn to show how various privacy metrics, can help your organisation further link privacy risks to operational and financial implications, as well as enable key business decisions. Delegates will walk away with a three-to-six-month roadmap of specific steps to take on what to measure and how, including how to communicate data in a way that effectively influences outcomes within an organisation.

What you will learn:
• Establishing a baseline and defining KRIs, KPIs and reporting metrics.
• How to design a privacy risk framework that allows for operational and strategic reporting.
• Specific use cases for which privacy metrics can be established.
• Real world examples of privacy metrics and their value to an organisation.

Additional registration fee required.

(Tags: Workshop, Consumer Privacy, Employee Privacy, Policy & Governance, Privacy Operations Management)

[Tuesday, 15 November, 9:00 – 13:00]
Privacy and Data Protection Law Forum

Privacy lawyers are as busy as ever, with no end in sight as new data protection and consumer privacy laws are adopted with increasing regularity around the world. Held in conjunction with Workshop Day sessions, the Privacy and Data Protection Law Forum is an information-packed, half-day programme presented by a distinguished and diverse panel of legal and data protection lawyers with deep experience in the field. As an opportunity for
legal minds throughout the industry to come together and focus on the profession, the forum is a way to network, learn and look to the future.

9:00 – 10:00
What EU & UK based Lawyers Need to Know About the DA & DGA

Claire Coleman, Group DPO, Revolut
Helena Koning, CIPP/A, CIPM, SVP, Assistant General Counsel, Europe DPO, Mastercard
Mark Taylor, Partner, Osborne Clark

10:00 – 10:30
The Essentials for Lawyers Assisting Clients on The AI Regulatory Requirements

Nathalie Laneret, CIPP/E, CIPM, VP Government Affairs and Public Policy, Criteo

As the AI Act is making its way through the legislative process, DPAs are increasingly publishing guidance on how data protection law applies to AI. This session will help you understand what is coming up for AI on the legislative front, what are DPA’s position on AI and how you can help your clients anticipate compliance by leveraging their data protection programme.

11:00 – 12:00
Class Action Litigation

Daniella Strik, Advocaat, Partner, European Divisional Lead Dispute Resolution, Linklaters
Tanguy Van Overstraeten, Partner, Global Head of Data Protection, Head of TMT IP Brussels, Linklaters

12:00 – 13:00
Regulators’ Panel

Ulrich Baumgartner, CIPP/E, Regional Leader, DACH, IAPP; Partner, Baumgartner Baumann
Florence Raynal, Deputy Director, Head of European and International Affairs, Commission nationale de l’informatique et des libertés
Isabelle Vereecken, Head of the EDPB Secretariat, European Data Protection Board
Michael Will, President, Bavarian State Office for Data Protection Supervision

In the era of the GDPR, organisations are in frequent contact with their supervisory authorities to get guidance, report breaches or register risky data protection impact assessments. What is the best way to build that relationship into a positive one? Will each regulator have a different method of communication, or will the European Data Protection Board help harmonise approaches? How can organisations expect lead authorities to work with fellow regulators in other member states? Get ready for a panel discussion that will explore these issues and more.

Additional registration fee required.

(Tags: Workshop; Privacy Law)

14:00 – 18:00

[Tuesday, 15 November, 14:00 – 18:00]
Adtech and Privacy: Prospects and Pitfalls

Alex Dixie, Partner, Head of AdTech Practice, London, UK, Bird & Bird

Most of today’s free consumer services are supported largely by online advertising revenues. The ecosystem that has evolved to support this business model is technical, complex and involves transferring many data types. Some of those data types are considered personal information by various state, federal and international laws, which at times contradict one another. Privacy professionals have a lot to figure out to be in legal compliance, and — perhaps just as importantly — to do right by their customers. These challenges stem from the interplay between the GDPR and ePrivacy rules; consent versus legitimate interests as a basis for processing; uncertain passage of the forthcoming ePrivacy Regulation; and the impact of ongoing regulatory complaints, investigations and enforcement actions. In this workshop, you will learn how to tackle your organisation’s internal challenges through practical and operationally focused panel discussions, case studies and conversation. Recent developments such as Google’s decision to deprecate third-party cookies in 2023, among other industry and regulatory breaking news, will be covered as well.

What you will learn:

• Key insights into the online marketing and advertising ecosystem, how it works and where it might be headed.
• Information about the laws that govern personal information management in this ecosystem.
• An understanding of what best practices exist for making policy decisions within your organisation.
• Hands-on, practical exercises that you can take back to the office and implement.

Additional Registration Fee Required.

(Tags: Workshop, Consumer Privacy; Enforcement; Infosecurity; Marketing; Privacy Enhancing Technology; Privacy Operations Management; Regulatory Developments)

Tuesday, 15 November, 14:00 – 18:00

Building a Global Privacy Programme That Performs

Marcin Czarnecki, CIPP/E, Senior Privacy Counsel, Prosus
Simon Hania, DPO, Uber
Monika Tomczak-Gorlikowska, CIPT, CPO, Prosus

Learn how to keep everyone happy — from customers to ICANN to international regulators — by building a global privacy programme that works. In this interactive workshop, privacy leaders will share their expertise on how they have managed privacy operations. You will learn about obtaining and sustaining executive buy-in, scoping the programme and privacy leader responsibilities, creating an achievable plan, matching a privacy programme to a corporate culture, assessing the effectiveness of the privacy programme, continuous programme improvement, governance and reporting, metrics and mistakes to avoid, responding to data breaches, techniques to show value and obtain funding, keeping abreast of outside resources, and career planning for the privacy team.

What you will learn:

• A roadmap for building a global privacy programme.
• Tactical implementation tips for automation efforts.
• Real stories of success on building and implementing a global privacy operations team.
• Tips on working with consumers, employees and regulators for privacy success.
• Practical tips for addressing issues in a global environment.

Additional registration fee required.

(Tags: Workshop, Policy & Governance, Privacy Operations Management)

[Tuesday, 15 November, 14:00 – 18:00]
Data Protection Agreements, Contractual Clauses & Accountability

Michael M. Pachinger, CIPP/E, Partner, SCWP Schindhelm

Data Protection Agreements become increasingly viable as they prove GDPR compliance, especially with regards to third party transfers. This workshop will outline how controllers may fulfil the principles of lawfulness, fairness and transparency by providing and securing such arrangements and drafting relevant (additional) clauses. Furthermore, selected topics of processing agreements, joint controller agreements and international agreements (SCC) will be outlined to show how margins can be used when designing the relevant agreements of finding additional clauses. Finally, a clear allocation of roles processor, controller and joint controllers is essential. In short: Drafting Data Protection Agreements entail questions of accountability, responsibility and liability — especially after “Schrems II.”

What you will learn:
• Data protection agreements as evidence of GDPR compliance.
• Standard Contractual & Additional Contractual Clauses.
• Accountability.
• Input on the draft and design of Processor, Joint-Controller and International Agreements.

Additional registration fee required.

(Tags: Workshop, Business of Privacy, Enforcement, Privacy Law, Trans-Border Data Flow)

[Tuesday, 15 November, 14:00 – 18:00]
Privacy Engineering Section Forum

With the rising tide of products and services collecting and processing personal data, the time for real data privacy solutions is here. The ever-closer connection between people, privacy and technology will be the focus of the next Privacy Engineering Section Forum, brought to you by the IAPP’s Privacy Engineering Section. This half-day event will take a nuts-and-bolts view of integrating privacy management and product development. Come for in-depth discussions and real-world examples of privacy management at work.

14:00 – 15:00
Privacy Engineering at Work: Implementing Privacy for Trust and Compliance

Nishant Bhajaria, Director of Privacy Engineering and Governance, Uber

Nishant Bhajaria will explain how you can use automation to make progress in compliance and then use that tooling to build user trust by offering choice and transparency. By doing
so, you will turn privacy into a business value and customer feature while improving efficiency and quality at your business.

**15:00 – 15:30**

**Introduction to PLOT4ai: a Privacy Library of Threats for AI/ML**

*Isabel Barberá, CIPP/E, CIPM, CIPT, FIP*, Privacy Engineer, Security Specialist, Rhite

In this session you will be introduced to PLOT4ai. PLOT4ai stands for Privacy Library of Threats for Artificial Intelligence. It is a threat modeling library inspired in LINDDUN that can help you build responsible AI systems. It contains a collection of 86 threats classified in eight categories. And it also provides a card game and a methodology to make threat modeling easier and more accessible for everyone working in the field of AI/ML. And best of all? PLOT4ai is open source and free for everyone to use!

**15:30 – 16:00**

**Privacy As A Key Pillar of Ethical and Responsible AI**

*Sray Agarwal*, Director, Fractal AI

AI models are prone to attacks and data leaks. There have been numerous instances of Privacy breach. We will talk about different stages of the data science life cycle where privacy needs to be implemented and various methods (input privacy, output privacy, model objective function privacy, etc.) of preserving privacy. To conclude, we will also look into privacy-preserving fairness and privacy monitoring.

**16:30 – 17:00**

**PETs in Practice: Possibilities and Challenges**

*Christian Zimmermann*, Privacy & Security Researcher, Bosch Research

Privacy-enhancing technologies (PETs) are important building blocks of privacy-preserving systems. This session takes a closer look at PETs and the potentials and challenges of applying them in practice.

**17:00 – 17:30**

**Engineering Transparency — A Techno-Legal Endeavor**

*Frank Pallas*, Senior Researcher, Technische Universität Berlin, Information Systems Engineering Research Group

Transparency is one of the core principles of privacy regulations around the world. In matters of technical implementations, however, it has gotten far less attention than other privacy principles so far. In this session, Frank Pallas will illuminate the foundations of transparency-related privacy engineering and the techno-legal tensions arising in this context. Based on select technologies, he will then present building blocks for engineering state-of-the-art, transparent, real-world systems and deviate possible regulatory implications.

**17:30 – 18:00**

**Closing Keynote: Privacy Threat Modeling: What, Why, How and What’s Next**
Privacy by design goes beyond the quick fixes that are often associated with it and requires a thorough upfront analysis of potential privacy issues in the system. Threat modeling has already proven its value for security and can be equally useful for privacy. This session will introduce privacy threat modeling basics, including some pointers on how to get started, and provide a summary of which modeling approaches can be used in different contexts.

Additional registration fee required.

(Tags: Workshop, Big Data; Business of Privacy; Ethics; Privacy Engineering; Privacy Enhancing Technology)

Wednesday, 16 November

[Wednesday, 16 November, 10:00 – 11:15]
Opening General Session

Alessandro Acquisti, Professor, Information Technology and Public Policy, Heinz College, Carnegie Mellon University

Acquisti gives an account of the evolutionary roots of privacy and how those roots may hold lessons for policies in the digital age.

[Wednesday, 16 November, 11:30 – 11:50]
A Customised SAP ILM Implementation Concept in Only 5 Days

Burkhard Hergenhan, Head of Data Management & Compliance, Natuvion GmbH

The Little Big Stage has been called entertaining, informative and many other things — but never boring. Find your way to the Exhibit Hall for these mini talks throughout the conference.

Sponsored by: Natuvion GmbH

(Tags: The Little Big Stage)

12:00 – 13:00

[Wednesday, 16 November, 12:00 – 13:00]
A New Direction — How the UK is Redefining Data Protection in the Global Context

John Bowman, CIPP/E, CIPM, FIP, Senior Principal, Promontory
Eleonor Duhs, CIPP/E, Partner and Head of Data Privacy, Bates Wells
Owen Rowland, Deputy Director, Head of Domestic Data Protection Policy, Department for Digital, Culture, Media and Sport

The UK left the European Union on 31 January 2020. Since then, the UK government has published plans to reform the UK’s data protection regime. Mechanisms are in place for the UK to confer adequacy decisions on an expanded range of third countries. A new Information Commissioner has been appointed with a mandate to enable people to use data
responsibly to achieve economic and social goals. Given the changes now in motion, how has the UK’s data protection framework changed? What innovations has the UK brought forward? How does UK data protection law now differ from EU data protection law? How does a company operating in both jurisdictions manage the differences? Our expert panel will answer all these questions and more in a clear and practical way.

**What you will learn:**
- How to explain the main changes to your organisation.
- Practical tips on how to manage UK and EU operations in a pragmatic way.
- Ensure that your compliance programme works for both jurisdictions.

(TAGS: Traditional Breakout, European Union, Government, Privacy Law, Trans-Border Data Flow)

[Wednesday, 16 November, 12:00 – 13:00]
**Controller, Processor, Joint Controller: Anything New Under the Sun?**

_Nana Botchorichvili, CIPP/E, Counsel, IDEA Avocats_
_Elise Malot, Head of Privacy Legal, Vinted_
_Olivier Matter, Head of International Cooperation, EDPS_

The concepts of controller, processor and joint controller are key as they determine who should do what under the GDPR. They have been subject to important case law from the Court of Justice of the European Union (CJEU) and guidance from the European Data Protection Board (EDPB) which clarified their meaning and application under the guidelines 07/2020, finalised on 7 July 2021. The panel aims to discuss how the concepts have since then been implemented in practice and the remaining challenges for organisations, including with respect to the management of the relationship between controllers and processors as well as joint controllers. It will also update on any legal or regulatory developments on these issues. Topics that will notably be addressed in this context: the Belgian DPA decision of 2 February 2022 on IAB Europe, EU Commission’s article 28 Standard Contractual Clauses (SCCs), and the French DPA’s guidance on the re-use of data by processors from their controllers.

**What you will learn:**
- Updates regarding the latest developments on these concepts and their impact on organisations.
- Possible solutions for framing controller/processor relationships as well as between joint controllers.

(TAGS: Traditional Breakout, Privacy Law, Regulatory Developments, Vendor Management)

[Wednesday, 16 November, 12:00 – 13:00]
**Cross-border Transfers Strategy to Non-Adequate Countries: Tricks and Solutions**

_Audrey Costes, CIPP/E, Global DPO, Webhelp_
_Anne-Cécile Colas, CIPP/E, CIPM, Group DPO, Sodexo_
_Fabrice Naftalski, CIPP/E, CIPM, Partner, Attorney at Law, Global Head of Data Protection, EY Société D’Avocats_
_Florence Raynal, Deputy Director, Head of European and International Affairs, CNIL_

(TAGS: Traditional Breakout, Privacy Law, Regulatory Developments, Vendor Management)
While the “Schrems II” decision and the subsequent EDPB guidance provided some direction on steps needed to transfer data to a non-EEA country, further analysis left many organisations still grappling with whether they could legally transfer data outside the EU. During the last 30 months, there have been many decisions and rulings from various national data protection authorities in the field of transfers, including Austria, Norway and France. Transfers outside the EU are still under scrutiny and subject to a slope of instability and movement. This panel will explore existing solutions to navigate among the different viewpoints and positions from regulators and lawmakers.

What you will learn:
- Solutions implemented by International Groups on the ground.
- What needs to be documented and how.
- What is expected and not expected in a TIA.
- To which extent BCRs, certifications and codes of conduct can help.
- To which extent the article 49 exception gate is effective and for which types of transfers.
- The progress of various multi-stakeholders’ initiatives (OECD, World Economic Forum, General Assembly, DPAs, etc.).

(Tag: Traditional Breakout, Enforcement, European Union, Privacy Law, Trans-Border Data Flow)

[Wednesday, 16 November, 12:00 – 13:00]
The Embrace of Privacy and Sustainability — How Privacy Became Part of ESG

Cecilia Álvarez, Director, Privacy Policy, EMEA, Meta
Vivienne Artz, Senior Data Strategy and Privacy Policy Advisor, Centre for Information Policy Leadership
Monika Tomczak-Gorlikowska, CIPP/E, CIPT, CPO, Prosus Group
Justin B. Weiss, CIPP/A, CIPP/E, CIPP/US, CIPM, FIP, Global Head of Data Privacy, Naspers and Prosus

Historically, privacy has not been considered an ESG issue, but in recent years there is an increased trend of including privacy disclosures in sustainability reporting and scoring. More and more often, privacy professionals work in alliance with sustainability teams to demonstrate how their organisations address privacy challenges and create a positive social impact. Traditionally, privacy has been addressed as part of the "Social" element of ESG, but most recently "Governance" can also include elements of a privacy programme. Therefore, the members of the privacy profession should understand the framework of this alliance and how privacy metrics can be leveraged to address the methodology of ESG scoring. Within this trend, privacy becomes a business governance imperative that goes 'beyond compliance" and is an essential part of building customer trust. As a result, the privacy profile and strategic importance is even further elevated. As part of this session, the panellists will discuss the practical implications of this alliance and provide the audience with insights as to their firsthand experience in addressing ESG expectations.

What you will learn:
- The growing importance of privacy as part of ESG agenda and reporting.
- The importance of privacy metrics for ESG scoring.
- How to navigate between the sustainability and privacy programmes’ objectives and lenses.

(Tag: Traditional Breakout, Ethics, Policy & Governance, Privacy Operations Management)
12:15 – 13:15

[Wednesday, 16 November, 12:15 – 13:15]

**A Data Intelligence and Automation-centric Approach for Privacy Management**

**Rehan Jalil**, CEO, President, Securiti

As organisations strive to meet their obligations across a myriad of regulations and an ever-increasing volume of data, they must transform their privacy management programmes to keep pace. While most companies started with spreadsheets and some evolved to survey-driven web tools, privacy leaders recognise these approaches provide limited accuracy and efficiency. What is needed is an automated approach based on real-time granular insights of an organisation’s data. This session will explore how major enterprises have implemented a modern privacy operations framework to address their privacy requirements; increasing accuracy, mitigating risks and reducing costs.

**What you will learn:**
- Best practices for harnessing a data-centric PrivacyOps approach to address privacy requirements.
- Tips for streamlining data mapping, assessments, data subject requests and breach management.
- How to effectively collaborate with privacy, security and governance teams.
- Real world lessons from leaders that have navigated the journey to automation.

*Sponsored by: Securiti*

(Tags: Traditional Breakout, Privacy Operations Management, Privacy Enhancing Technology)

[Wednesday, 16 November, 12:15 – 13:15]

**Consumer Perspectives on Privacy and Implications for Business Growth**

**Russ Howe**, VP EMEA, Ketch

People’s heightened awareness of their data privacy and expectations of responsible data practices will shape privacy programmes more than regulations. What can we learn by listening to the people behind the data? In this session, we will unveil the latest research on consumer perspectives on data privacy and businesses’ data practices, while measuring impact on the bottom line. We will explore what it means to have responsible data practices and discuss important trends and innovations to future-proof your privacy programme. We will also recommend a practical framework for building a privacy programme that builds trust with consumers and uses data to drive business growth, in addition to managing compliance and reputational risk.

**What you will learn:**
- The value consumers place on their data privacy, relative to other shared values like sustainability and diversity.
- The impact of responsible data practices on top-line growth and brand preference.
- Where businesses are falling short today and practical advice for building capability maturity into your privacy programme.
EU Strategy for Data’s DGA, DSA, DMA, NIS2: From Policy to Practice

Karolina Mojzesowicz, Deputy Head of Unit Data Protection, European Commission
Isabelle Roccia, Managing Director, Europe, IAPP
Tanguy Van Overstraeten, Partner, Global Head of Data Protection, Head of TMT IP Brussels, Linklaters

In February 2020, the European Commission unveiled the “European Strategy for Data.” Fast-forward to November 2022, at least four new pieces of legislation have entered into force: the Digital Governance Act, the Digital Services Act, the Digital Markets Act, the revised Network and Information Security Directive, and a few more on the way. None of these texts address privacy or data protection straight on; they deal with data sharing and reuse of data, online content management, competition and cybersecurity. Yet, they are landing on privacy practitioners’ desks as they become applicable and need to be implemented.

What you will learn:
- How the DGA, DSA, DMA, NIS2 affect privacy and data protection compliance programmes.
- How experts recommend organisations tackle the new requirements.
- Some of the compliance challenges foreseen (in terms of processes, competences, impact on business models and enforcement).
- How to prepare for the next wave of legislative changes and new rules (e.g. data spaces, certification).

The Future of Data Starts Today and Not Tomorrow

Saz Kanthasamy, CIPP/E, CIPM, FIP, Principal Researcher, Privacy Management, IAPP
Mark Thompson, CIPP/E, CIPM, CIPT, FIP, Chief Strategy Officer, IAPP
Gemma Witham, CPO, SkyScanner

Every second, minute and hour of everyday of every year, humanity is collecting, using and storing more data than ever before. But where did this journey start and where could it end? In this session we will look at the “3 Vs”; how the Volume, Velocity and Variety have changed since the first structured record was created. We will explore how continuous and discontinuous innovations and advancements in human understanding have impacted the 3 Vs over time. We will explore what this could look like in the future and consider the inflection point at which the sheer scale of the 3 Vs means that a loss of data would cause irrevocable harm to an individual.

What you will learn:
- How the volume, velocity and variety of data have changed over time.
- What the future may hold for the 3 Vs of data.
- The risks that need to be considered now and in the future for privacy professionals.
- How human innovations have impacted the 3 Vs in the past and how they may impact it in the future.
As data protection professionals’ heads spin trying to keep up with technological advances and ever-changing legislative landscapes, we hit the pause button — at least for a few moments — to reflect on how cutting-edge organisations of all shapes and sizes are weaving privacy education into their ethos. Set against the backdrop of emerging privacy considerations that evolve daily across a multitude of industries, our panellists share their firsthand experiences of leading and going beyond a compliance-centric approach to creating a true culture of privacy for both their own teams and the clients they serve.

**What you will learn:**
- Hands-on suggestions and ideas for how to build and enhance your organisation’s privacy IQ using real-life case studies.
- Recommendations on winning support for your programme both within, and outside, of the data protection office, including the development of privacy champions.
- Examples of how different organisations embed privacy by design into their company’s DNA through their unique approaches to privacy and data protection education and awareness.

**Data Regulation Ramps Up in Europe: The AI Act, Data Act, and Data Governance Act**

Linda Thielová, CIPP/E, CIPP/US, CIPM, FIP, Head of Privacy Center of Excellence, DPO, OneTrust

The Little Big Stage has been called entertaining, informative and many other things — but never boring. Find your way to the Exhibit Hall for these mini talks throughout the conference.

*Sponsored by: OneTrust*
Talent attraction and retention require companies to be more and more innovative. Data helps considerably in this regard. Artificial intelligence brings HR into a new dimension. Recruitment interviews can be carried out by virtual assistant, and AI can be used to anticipate and determine career paths, predict employees’ attrition and support retention. While the possibilities of AI in the HR domain seem endless, companies need to take into account both the data protection and artificial intelligence regulatory requirements. In practice, data protection constraints need to be taken into account from the design phase of any project applying artificial intelligence for the HR function. The selection of any third-party provider of AI solution for HR would need to be made with the utmost care. In this context, it is important for privacy specialists to team up with HR function to draw the line as to how AI can be deployed in a compliant way to support HR objectives while making sure HR can leverage opportunities offered by AI.

**What you will learn:**
- How to ensure compliance with the data limitation principle when AI benefits from more rather than less data.
- How to ensure data subjects are well informed about the processing of their personal data, while AI may be synonymous with endless possibilities of processing activities.
- Tips on how to best support HR in the different phases of their projects to leverage AI.

(Tags: Traditional Breakout, Employee Privacy, Human Resources, Privacy Law)

[Wednesday, 16 November, 14:30 – 15:30]

**Civil GDPR Litigation: Defense Against (Mass) GDPR Damages Claims**

**Oliver Draf**, CPO, Volkswagen AG, Germany
**Tim Wybitul, CIPP/E**, Partner, Latham & Watkins

Most practitioners associate the GDPR with high fines. But the actions of data protection authorities are increasingly prompting specialised plaintiffs' lawyers and litigation financiers. The goal of these players is the mass commercialisation of GDPR damage claims, for example after major data breaches. They are therefore actively marketing themselves to potential plaintiffs. For companies, handling such an incident involves considerable effort. In this interactive session, Tim Wybitul and Dr. Oliver Draf explain the current case law on GDPR damages and the legal basis of the claims. One focus is on the numerous referrals from various European courts to the CJEU. Germany may very well be considered the spearhead of GDPR plaintiffs within the EU. Therefore, the speakers use German court rulings as a blueprint to explain current issues. Finally, Tim Wybitul will provide insights and experiences from successfully defending thousands of mass GDPR-claims spanning multiple jurisdictions. Speakers will also provide concrete recommendations for action.

**What you will learn:**
- How claiming GDPR damages is being turned into a business model by legal service providers.
- How companies can successfully defend themselves when facing GDPR claims.
- A comprehensive understanding of the dynamic legal framework and court rulings regarding GDPR claims.

(Tags: Traditional Breakout, Business of Privacy, Consumer Privacy, Data Breach, Employee Privacy, Enforcement)

[Wednesday, 16 November, 14:30 – 15:30]
A Conversation on Privacy and National Security: The PCLOB’s Role

Sharon Bradford Franklin, Chair, U.S. Privacy and Civil Liberties Oversight Board
Alan Charles Raul, Partner, Sidley Austin

See the Chair of Privacy and Civil Liberties Oversight Board, Sharon Franklin in conversation with Alan Raul, Privacy and Cybersecurity partner at Sidley Austin LLP and former Vice Chairman of the PCLOB. Understand the PCLOB’s role in advising and overseeing the President and U.S. national security agencies regarding privacy and civil liberties. PCLOB will likely play an indispensable part in helping address the conflicts and uncertainties on transatlantic data flows arising from decisions of the Court of Justice of the European Union in the “Schrems II” litigation.

What you will learn:
• The PCLOB’s authorities, responsibilities and powers regarding privacy and national security.
• How the protection of privacy and civil liberties can and must be balanced with national security.
• If the PCLOB will be involved in addressing the privacy interests of EU and other non-U.S. Persons.
• The role the PCLOB will play in any successor to Privacy Shield.

(Tags: Policy & Governance; Regulatory Developments; Trans-Border Data Flow)

[Wednesday, 16 November, 14:30 – 15:30]
Cookies and Data Sharing: The Impact of Enforcement Actions

Moderator: Christian Leuthner, CIPP/E, Partner, Reed Smith
Robert Gillis, Head of Privacy Legal, EMEA (Acting), Citi
Julie Rubash, Chief Privacy Counsel, Sourcepoint
Harneesh Sangra, CIPP/E, DPO, Boots

Recent decisions by EU supervisory authorities, EDPS and courts in Member States will have a practical impact on how your organisation uses cookies on websites. We would like our panellists (brands and a CMP provider) to share how they are addressing the issues raised by the recent enforcement actions, specifically on the following: impact of the recent enforcement actions on the rejection of cookies, multijurisdictional strategy, data sharing of information collected by cookies and similar technologies with third parties and transfers of data collected by cookies to third countries.

What you will learn:
• Updates to the records of processing to add cookie-related data due to recognition of it as personal data.
• Due diligence and third-party vendor management, when it comes to website management, hosting, payment providers and CMP providers.
• Considerations if cookie data can be processed within the EU/UK.
• Where cookie data is transferred to third countries, consider new SCCs (UK/EU).
• How to conduct a transfer impact assessment to see if such transfers provide sufficient protection to the personal data from the government access perspective.

(Tags: Traditional Breakout, European Union, Marketing, Trans-Border Data Flow, Vendor Management)
[Wednesday, 16 November, 14:45 – 15:45]

**Drive Growth with European Values: Security, Privacy & Resilience in the Cloud**

**Moderator: Arnaud David**, Director European Affairs, Amazon Web Services

According to a new study by Public First, the European Commission’s (EC) Digital Decade could unlock an additional €2.8 trillion in economic value. Realising the EC's vision for 75 percent of EU companies to use cloud services by 2030 requires sustained, collective focus and cooperation across the public and private sectors. In this session, learn how to work together to help Europe unlock its digital ambitions. Discover how cloud computing is critical enabling technology for growth in Europe, not only to drive innovation, but also to meet the highest levels of security, privacy and resilience.

**What you will learn:**
- How cloud computing is critical enabling technology for growth in Europe.
- How European customers enhance data privacy using cloud services.
- How cloud computing can enable European organisations to drive innovation while helping them meet the highest levels of security, privacy and resilience.

*Sponsored by: AWS*

(Tags: Traditional Breakout, Privacy Enhancing Technology, European Union)

[Wednesday, 16 November, 14:45 – 15:45]

**Global Privacy State of Play**

**Gabriela Zanfir-Fortuna**, Senior Counsel, Future of Privacy Forum

Privacy and data protection laws have been adopted at an incredible pace in the past years, around the world. From Brazil, to China, to Kenya, and very recently Indonesia - major jurisdictions across continents now have comprehensive data protection laws in place. Join this session to understand what are the key global trends in data protection and privacy regulation, how does enforcement look like, what are the key compliance challenges and whether there are new barriers to international data flows.

**What you will learn:**
- Understand latest data protection developments in key jurisdictions from Latin America, Asia and Africa
- Identify compliance challenges when processing personal data across continents
- Map the underlying trends of a developing global data protection and privacy landscape

(Tags: Traditional Breakout, Regulatory Developments)

[Wednesday, 16 November, 14:45 – 15:45]

**Globalising Privacy Strategy in the Life Sciences Sector: What the Health!**

**Patrice Navarro**, Partner, Hogan Lovells

This session will address the various difficulties to overcome for controllers in the healthcare and life sciences sector who need to comply and operate at a global level. Harmonising the approach is necessary, but local laws create a conundrum to solve. Especially in our new world where more and more innovative medical and healthcare practices are developed.
Remote and digitalised approaches are multiplying for the benefit of us all but require implementing innovative privacy solutions to keep protecting personal data and data subjects.

**What you will learn:**
- Understand the issues while juggling with multiple regulatory frameworks.
- Create an efficient global approach despite these issues and the recent raise in data localisation concerns.
- Leave the session with a key actions plan.

(Tags: Traditional Breakout, Big Data, Healthcare Privacy, Policy & Governance, Privacy Operations Management, Trans-Border Data Flow)

**16:00 – 17:00**

[Wednesday, 16 November, 16:00 – 17:00]

**Accelerate Your Company’s Global Compliance Programme**

**Benjamin Baeuerle**, Head of Data Privacy Legal and Strategies, Siemens AG  
**Marcela Ejnisman**, Partner, Tozzini Freire Advogados  
**Kristen Fang**, DPO, Siemens  
**Julia Kaufmann, CIPP/E**, Partner, Osborne Clarke Germany

The GDPR not only established a level playing field for data privacy in the European Union but serves as a role model for data privacy laws globally. China just recently introduced its new Personal Information Protection Law with many GDPR-like provisions; the Brazilian LGPD, enacted in 2018, broadly aligns with GDPR principles; India is about to adopt its first Privacy Act; several U.S. states have adopted State Privacy Laws, and other countries are following this trend. How does this impact group-internal data sharing and roll outs of global IT applications as the requirements are similar but far from identical and fully consistent? How can multinational companies adopt a group-wide privacy compliance programme that is aligned with the requirements of the colourful global privacy landscape? In this session we share our experience gained in multinational companies while managing these challenges.

**What you will learn:**
- A summary of recent developments in global privacy landscape.
- Suggestions for the development of group-wide privacy compliance programmes.
- Pragmatic solutions for group-internal data sharing in light of unharmonised national privacy law requirements.

(Tags: Traditional Breakout, Policy & Governance, Privacy Operations Management, Regulatory Developments)

[Wednesday, 16 November, 16:00 – 17:00]

**Anonymisation Techniques: Defining the Borders of the GDPR**

**Nataliia Bielova**, Researcher, CNIL  
**Xavier Darrigol**, Co-Founder, Retency  
**Etienne Drouard, CIPP/E**, Partner, Hogan Lovells

The EDPB is working in 2022 on a new Recommendation on anonymisation techniques, eight years after the first Article 29 WP216 Recommendation 05/2014 was issued in April 2014. Under the former EU Data Protection Directive 95/46, anonymisation techniques had
been smoothly debated, despite several fierce litigations in 2009, 2015 and 2017. Since the GDPR, tens of alleged anonymisation techniques have been submitted to EU DPAs. In France, only two of them were officially certified by the CNIL. Why? In which contexts? How can anonymised data analytics solutions preserve some data value without GDPR boundaries? This panel will provide regulatory, technical, business and practical insights, as well as use cases of valid anonymisation techniques under the GDPR, which are in use in the insurance, banking, transportation, smart cities, retail shopping, digital advertising and life science industries.

What you will learn:
- An understanding of nuances and various regulatory approaches defining pseudonymisation and anonymisation techniques within the EU.
- Use cases describing interactions between data value and data anonymisation.
- Demystifying technical aspects of anonymisation and building bridges between legal, technical and business approaches.

(Tags: Traditional Breakout, Consumer Privacy, Identity Management, Privacy Engineering, Privacy Enhancing Technology, Regulatory Developments)

[Wednesday, 16 November, 16:00 – 17:00] Ethical and Trustworthy Artificial Intelligence: From Theory to Practice

Anna Buchta, Head of Unit, Policy and Consultation, EDPS
Tom De Cordier, Partner, Tech and Data Law, CMS
Helen Hulsker, CIPP/E, Senior International Legal Counsel, Randstad

Businesses and governments increasingly use artificial intelligence to automate high-impact decisions such as rehabilitation and prison sentence decisions, legal decisions, etc. As a result, ethical artificial intelligence emerged. Ethical AI aims to make fair decisions that respect ethical values. Ethical AI is part of trustworthy AI. Trustworthy AI includes human agency and oversight, technical robustness and safety, privacy and data governance, transparency, societal and environment well-being and accountability. In this session, you will learn what ethical and trustworthy AI actually is and how to put responsible AI into practice. We will also discuss how the GDPR and the EU Commission’s proposed AI Regulation contribute to responsible AI. The panellists will take a 360-degree look at responsible AI from a regulator’s perspective, a practitioner’s perspective and a legal perspective.

What you will learn:
- The emerging frameworks for building responsible AI.
- What exactly is ethical and trustworthy artificial intelligence.
- Practical tips and tricks on how to put responsible AI into practice.
- The risks if you get it wrong.

(Tags: Traditional Breakout, Big Data, Consumer Privacy, Employee Privacy, Ethics, Regulatory Developments)

[Wednesday, 16 November, 16:00 – 17:00] The One and Only Intercompany Privacy Agreement?

Lydia Faltas, CIPP/E, CIPP/US, Director, Global Privacy, Cognizant
Marcus Sinha, Director, Data Protection; European DPO, Amgen
Florian Thoma, CIPP/E, CIPP/US, CIPM, FIP, Senior Director, Global Data Privacy, Accenture

With new laws and regulations everywhere, new challenges arise for us privacy professionals: how do we implement intercompany privacy agreements efficiently and effectively in our organisations as we need to consider various laws, roles, domestic and cross-border frameworks as they keep changing? What started in the EU and U.S. is now ubiquitous (e.g., BCR implementation, SCCs, HIPAA, cross border arrangements, processing agreements)? How do we implement and maintain just one framework that covers most of the relevant content instead of administrating a dozen or more sets of contracts for sometimes hundreds of entities? How do you stay a strategic privacy pro and do not risk becoming the chief paperwork administrator?

What you will learn:

- Inspiration and guidance for simplifying your organisation's contractual privacy landscape.
- What is feasible and where you need to address remaining issues.

(Tags: Traditional Breakout, Policy & Governance, Privacy Law, Privacy Operations Management, Trans-Border Data Flow)

16:15 – 17:15

[Wednesday, 16 November, 16:15 – 17:15]
Applying the Best Interests of the Child Principle in Practice

Cecilia Álvarez, Director, Privacy Policy, EMEA, Meta

“The best interests of the child” is a central principle of the UN Committee on the Rights of the Child. Since then, a number of regulatory instruments on the protection of children in the digital world are underpinned by the best interests of the child in Europe and beyond. Applying this dynamic principle in practice requires carefully balancing the various rights of the child and consideration of the diverse issues at stake, namely privacy and safety. This panel invites speakers representing varying expertise to examine the best interests of the child and explore how it can be achieved in practice. In particular, the session will delve into how the best interests of the child can be applied to implementing safety measures such as age assurance.

What you will learn:

- Diverse approaches taken by different sectors and fields to operationalise the principle.
- Interplay between data protection, safety and other pertinent areas when embedding the principle in the design of digital services.
- Application of the principle to practical age assurance solutions.

Sponsored by: Meta

(Tags: Traditional Breakout, Children’s Privacy, Policy & Governance)

[Wednesday, 16 November, 16:15 – 17:15]
Automated Decision-making and Profiling: Lessons from Court and DPA Decisions
Sebastião Barros Vale, EU Policy Counsel, Future of Privacy Forum
Ruth Boardman, Partner, Co-head, International Data Protection Practice, Bird & Bird
Simon Hania, DPO, Uber
Gintare Pazereckaite, Legal Officer, EDPB

Since the EDPB clarified the GDPR’s concepts of “profiling” and “automated decision-making” through the endorsement of the 2018 Article 29 Working Party guidelines, judges and regulators across the EU have been called to apply them in real-life cases. Building on a comprehensive case-law report published by FPF, this session will explore their most impactful decisions—like the Dutch rulings regarding Uber’s alleged algorithmic management of drivers and the Spanish DPA’s sanctions against Caixabank—and how the pending cases before the CJEU can clarify the interpretation of key provisions. When can a decision be considered “based solely on automated processing” and have the types of effects covered by Article 22 in the GDPR? How does the GDPR apply Automated Decision-making which does not meet the Article 22 threshold? How much does the GDPR already regulate AI systems covered by the proposal for an AI Act?

What you will learn:
- An overview of existing enforcement precedents of Article 22 and its related transparency and access provisions in the GDPR.
- Valuable insights on how to assess whether delegates’ planned or implemented AI systems or products are covered by Article 22, as well as on the information that should be provided to data subjects in cases of profiling.
- The broad extent to which the GDPR is applying Automated Decision-making which does not meet the Article 22 threshold.

(Tags: Traditional Breakout, Employee Privacy, Enforcement, European Union, Privacy Research, Regulatory Developments)

[Wednesday, 16 November, 16:15 – 17:15]
DMA, DSA, DA, DGA, AI Act: How to Navigate a Soup of New EU Data Regulations

Moderator: Cédric Burton, CIPP/E, Partner, Co-Chair Privacy and Cybersecurity Practice, Wilson Sonsini Goodrich & Rosati
Caroline Louveaux, CIPP/E, CIPM, CPO, Mastercard
William Malcolm, Senior Director, International Privacy and Consumer Protection, Google

This session will help participants navigate the complex web of (drafted) new data laws in the EU. Panelists will discuss implications for large tech players, companies that engage with them, and other businesses offering data-related products and services. Come learn how to build a compliance programme that meets the new requirements. Panellists will also discuss the interplay with the GDPR and the enforcement of the new rules.

What you will learn:
- Key principles of the DMA, DSA, DA, DGA and AI Act.
- Implications for businesses.
- Interplay with GDPR.

Sponsored by: Wilson Sonsini Goodrich & Rosati

(Tags: Traditional Breakout, Regulatory Developments, Policy & Governance)

17:30 – 18:30
[Wednesday, 16 November, 17:30 – 18:45]

**Enforcement in Europe from the Angle of National Case Law**

**Moderator:** Kate Colleary, CIPP/E, CIPM, Country Leader, Ireland, IAPP; Director, Pembroke Privacy  
Ulrich Baumgartner, CIPP/E, Regional Leader, DACH, IAPP; Partner, Baumgartner Baumann  
Yann Padova, Country Leader, France, IAPP; Partner, Baker McKenzie  
Rocco Panetta, CIPP/E, Country Leader, Italy; Managing Partner; Chairman, IAPP; PANETTA Law Firm; PTP Privacy Tech Professionals  
Jeroen Terstegge, CIPP/E, CIPP/US, Country Leader, Netherlands, IAPP; Managing Partner, Privacy Management Partners  
Eija Warma-Lehtinen, CIPP/E, Country Leader, Nordics, IAPP; Partner, Data Protection and Privacy, Castrén & Snellman

In recent months, several court rulings have challenged enforcement decisions from Supervisory Authorities across Europe, underlining the importance of the judicial system in the European interpretation and enforcement of the GDPR. These rulings spun from questioning fine calculation in Italy to the interpretation of core GDPR concepts, such as legitimate interest in The Netherlands. During this session, the IAPP’s country leaders from Finland, France, Germany, Italy, Ireland and The Netherlands will discuss the importance of national case law on enforcement in their respective markets. They will explain differences and commonalities of national courts’ systems and approaches to privacy and data protection enforcement across countries, and their implications for pan-European enforcement.

**What you will learn:**
- Areas of focus of national litigation, trends and patterns.  
- Relevant past rulings and upcoming cases to monitor.  
- Impact of national litigation on Supervisory Authorities’ enforcement at national and at pan-European level.

(Tags: Traditional Breakout, Enforcement)

[Wednesday, 16 November, 17:30 – 18:30]

**Europe’s Quest for Digital Sovereignty: What it Means for Data Protection**

**Paul Nemitz,** Principal Adviser on Justice Policy, European Commission  
Lokke Moerel, Senior Of Counsel, Morrison & Foerster; Professor, Global ICT Law, Tilburg University

The EU feels the threat of what is coined ‘tech colonialism' of the U.S. and China. The EU member states are increasingly dependent on the digital infrastructure of a handful of dominant market players, while most European data reside in foreign clouds. The sovereignty concerns have led to a U-turn in EU policy and restoring Europe’s “digital sovereignty” is now a core ambition of the European Commission. But how can they achieve this in a time where digital technologies have become a battleground for the race for global leadership between the U.S. and China (aka the tech cold war)? Both the U.S. and China regularly draw the national security card to justify stricter export controls of critical technology, while bringing manufacturing back to their countries and banning export of important data. With the EU Digital strategy, the EC is aiming to pave a third way, and avoid falling into the trap of tech protectionism. Flagship initiatives are the so-called
European Data Spaces (bringing together EU data of specific industry sectors in order to unlock their value for EU innovation) and the GAIA-X project (achieving interoperability between cloud offerings to achieve the required scalability for AI-related innovations). All initiatives will impact data protection, as well as how transfers under “Schrems II” are considered. We will discuss the threats to EU digital sovereignty in order to better understand the EU Digital Strategy based on open data, open ecosystems and open source, and its disruptive impacts, which—as any regulation—bring new requirements but also opportunities for innovation.

**What you will learn:**
- What are the threats to EU digital sovereignty.
- How does the EU aim to restore digital sovereignty, and how do the policy initiatives fit together.
- What does it mean for data transfers.
- If the EU data strategy be aligned with GDPR.
- What is expected of privacy professionals and how can they advise the business.

(Tags: Traditional Breakout, Big Data, Cloud Computing, European Union, Policy & Governance, Trans-Border Data Flow)

[Wednesday, 16 November, 17:30 – 18:30]
**I Say “High,” You Say “Low” — Risk Assessments Under the Proposed AI Act**

*Tobias Bräutigam, CIPP/E, CIPM, FIP*, Adjunct Professor, Uni Helsinki; Senior Counsel, Head of Data Protection, Bird & Bird Finland

*Erin Gülbenkoğlu*, Data Scientist, Wolt

*Monika Tomczak-Gorlikowska, CIPP/E, CIPT*, CPO, Prosus Group

The session will look at the proposed AI Act of the European Commission in context of the processing of personal data and risk assessments. We will start by giving an overview of the Act (as it will stand) and then compare it to the existing models of risk assessment, in particular under the GDPR. The Act foresees different levels of risk (unacceptable, high or low), which go along with different measures controllers need to take. Is the risk assessment methodology largely aligned between data protection and the draft AI Act? Are the AI risk labels assigned in a way that makes it simple for organisations to differentiate between unacceptable, high and low? How should the initial triage be construed to avoid AI projects becoming overly burdened or slipping through the net? These are all questions that will need to be addressed by organisations involved in developing and/or implementing AI in their business models. Subsequently, we will look at two case studies from two companies in different business areas to illustrate the above challenges. How are they implementing risk assessments and what role does the processing of personal data play? What can be considered as the end goal to achieve compliance with both the draft AI Act and GDPR?

**What you will learn:**
- The AI Act and what kind of risk assessments are needed.
- How the AI Act interacts with the GDPR.
- How two different companies are approaching the issue.

(Tags: Traditional Breakout, Big Data, Business of Privacy, European Union, Privacy Operations Management, Regulatory Developments)

[Wednesday, 16 November, 17:30 – 18:30]
**Operationalising Privacy by Design to Strengthen GDPR Compliance**
Moderator: Katharina Koerner, CIPP/US, Senior Fellow for Privacy Engineering, IAPP
Nishant Bhajaria, Director of Privacy Engineering and Governance, Uber
Laurits Ketscher, CIPP/E, Cyber Engineering Manager, IKEA
Srinivas Poosarla, CIPP/A, CIPP/E, CIPP/US, CIPM, CIPT, FIP, Sr. VP and Group Chief Privacy Officer, Infosys

In recent years, the proliferation of digital apps has given private and public corporations a disproportionate ability to glean data deriving insights about us, causing significant impact to our decisional autonomy. For a DP Office perennially starved by resources, there is no way to address privacy assurance by inspection at the scale this is transforming organisations all over the world. Instead, privacy must become incorporated in the functional design by development engineers and facilitated by privacy engineers. This is particularly important given the increasing digital convergence, innovation in emerging tech, and most development adopting the Agile methodology.

What you will learn:
- The realisation that PbD is not a fad. It is indispensable for achieving privacy assurance both for compliance and privacy as a differentiator in today’s digital world.
- What PbD involves and how enterprises can tailor their approach to their needs and achieve a positive sum game.
- How privacy engineering can be integrated with application development to make it part of an organisation’s culture.
- Various PbD strategies, particularly in use cases adopting emerging tech.

(Tags: Privacy Engineering, Privacy Enhancing Technology, Privacy Operations Management)

[Wednesday, 16 November, 17:30 – 18:30]
The Evergreen Privacy Programme — Myth or Reality?

Kate Brimsted, UK Data Privacy and Security Lead, Bryan Cave Leighton Paisner
Delphine Charlot, CIPP/E, CIPM, Senior Managing Counsel, Privacy and Data Protection, Mastercard
Anne-Cécile Colas, CIPP/E, CIPM, Group DPO, Sodexo
Amy de La Lama, CIPP/US, Chair, Global Data Privacy and Security, Bryan Cave Leighton Paisner

With contributions from seasoned industry and private practice experts, this panel session will home in on the Big Questions for every global privacy programme: where do you start? How to triage the competing issues, working out how much is universal and how much is organisation specific? How to make the best of finite resources, experiences with external vendors and keeping up the momentum (the Privacy Programme is never "done" as we know). We will also highlight themes in legal and regulatory changes already having or are about to have an impact on an organisation's privacy programme, including international transfers, data security breaches and data localisation.

What you will learn:
- Practical lessons learned from implementing global privacy programmes.
- Main trends and developments to watch out for in the privacy space which are expected to have a significant impact over the coming months/years.
Perspectives on the Latest US Privacy Developments

**Moderator:** Cobun Zweifel-Keegan, CIPP/US, CIPM, Managing Director, D.C., IAPP
**Stacey Gray, CIPP/US,** Senior Director for U.S. Policy, Future of Privacy Forum
**Maneesha Mithal,** Partner, Privacy and Cybersecurity, Wilson Sonsini Goodrich & Rosati

It has been a busy year for privacy and data protection in the United States, with important developments in Congress, a new rulemaking from the top privacy regulator, and a plethora of state-level legislative developments. To help separate the signal from the noise for a European audience, this panel features a balanced mix of on-the-ground expert voices who will explain the implications of shifting privacy best practices. The roundtable discussion will focus on the newest compliance insights from recent laws and regulatory enforcement and explain how proposed legislation and regulatory guidance could shape data protection norms as part of the global policy conversation.

**What you will learn:**
- Insights on the evolving foundation of data protection and privacy for anyone who does business with U.S. organisations or processes personal data of U.S. data subjects.
- Perspectives from leading U.S. policy and regulatory voices.
- An understanding of how current regulatory trends will shape future practices, including emerging areas such as artificial intelligence.

Deciphering Approaches to Enforcement in France, Europe and the U.S.

**Karin Kiefer,** Director, Rights Protection and Sanctions Directorate, CNIL
**Gwendal Le Grand,** Head of Activity for Enforcement Support and Coordination, EDPB
**Judicaël Phan,** VP Digital Trust, DPO, Contentsquare
**Noah Joshua Phillips,** Commissioner, FTC

Over the last years, the Data Protection Authorities have received more and more complaints and have increased the amount of their fines. They have carried out online and onsite inspections on many topics (e.g., marketing, cookies, AI, HR, sensitive data and children’s data). This roundtable will be a great opportunity to understand the decisions of the CNIL, the EDPB and the FTC and to discuss their enforcement actions plans.

**What you will learn:**
- An understanding of the past, present and future of enforcement actions of the CNIL, the EDPS and the FTC.
- How to anticipate the enforcement trends in France, Europe and the U.S.
- Gain strategy and identify best practices for avoiding the class actions and the sanctions.
Designing for Privacy in the Physical World

**Hubert Beroche**, Founder, Urban AI; Co-Founder, President, AI for Tomorrow  
**Sarah Gold**, CEO, Founding Partner, Projects by IF  
**Jacqueline Lu**, Co-Founder, Helpful Places; Data Lead, Mozilla Foundation  
**Lauren Reid, CIPP/E, CIPP/US, CIPM, FIP**, President, The Privacy Pro

As the smart city is gaining ground all over the world, people are increasingly worried about their privacy in the physical world. As sensors and facial recognition technology become cheaper and more widely available, how do we know who is using it and why? How can organisations build trust and show accountability in an environment where space is limited, and people are only passing by? For those organisations who are willing to bridge the gap with users, this session will discuss the challenges they will encounter when trying to develop an effective communication, and how design can help them overcome these challenges.

**What you will learn:**
- How design principles can guide infrastructure choices to promote a privacy by design approach.
- How design can be used to communicate with the public on how their data is used.

The AI Act: The State of the Art

**Brando Benifei**, Member, European Parliament  
**Alberto Di Felice, CIPP/E**, Director for Infrastructure, Privacy & Security Policy, DIGITALEUROPE  
**Fanny Hidvègi**, European Policy Manager, Advocacy Director, Access Now  
**Rocco Panetta, CIPP/E**, Country Leader, Italy; Managing Partner; Chairman, IAPP; PANETTA Law Firm; PTP Privacy Tech Professionals

What is the current status of the AI Act? What is the European Parliament's position? Does the text guarantee the necessary space for companies to innovate while safeguarding the fundamental rights of citizens? What role will the Data Protection Authorities play? How will the role of the DPO change, if at all? We will answer these questions with representatives of European institutions, civil society and businesses.

**What you will learn:**
- The state of the art of the AI Act.  
- The unresolved issues according to civil society.  
- Views in the industry and practitioners.
The Imbalance of Power Between Controllers and Cloud Service Providers

Jorge Alejandro Carrillo Ugalde, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP, Czech Board Member, (ISC)^2
Petruta Pirvan, CIPP/E, CIPP/US, CIPM, FIP, Senior Privacy Principal Consultant, Wrangu

Cloud services are scalable and cost-effective computing-service models, providing processing and storage services. Yet, the cloud services inherently conflict with the application of the law where the provider role is fixed. The applicability of the legal status to the cloud service context is hard to map out because the cloud service contains many characteristics, such as designs of virtualised infrastructure shared among multiple users, including several add-on service providers. The key legal problems of cloud service are the inability to influence the design of controls and complexities to understand their privacy policies on transparency. This session is about the operational ambiguities of the division of responsibility where a processor has the power to dictate the conditions of the services. The Article 29 WP maintains that the standard of responsibility should not be lowered on the ground of economic imbalance. But is this feasible in practice?

What you will learn:
- Understand the challenges of take-it-or-leave-it service level agreements (SLAs), which seems to offer an already structured cloud with little to no room for controllers to negotiate the contractual terms.
- Evaluation techniques to address privacy risks when the cloud provider/processor exploits its power over the controller's data and the challenges deriving from an ambiguous legal status of the parties.

(Tags: Traditional Breakout, Cloud Computing, Privacy Law, Regulatory Developments, Vendor Management)

[Thursday 17 November, 9:15 – 10:15]

Data Retention 101: Building an Automated Retention Programme

Heather Federman, CIPP/US, CPO, BigID
Martin Macke, CIPP/E, CIPM, FIP, Global Privacy Director, ManpowerGroup

Many organizations over-retain data, while most consist of personal and sensitive data. Even with regulatory enforcement, it is still a struggle to implement a data retention strategy consistent with compliance requirements. As a result, organizations must shift toward automated retention policies that quickly remediate violations. The goal is to reduce cost, improve efficiency and minimize risks to the privacy and security of personal data.

What you will learn:
- How to overcome data retention challenges
- Best practices for designing a data retention program
- How to introduce automation, risk management, and scale

(Tags: Traditional Breakout, Privacy Operations Management, Business of Privacy)

[Thursday 17 November, 9:15 – 10:15]

Enforcement Cooperation: A Look Behind the Scenes
Moderator: Caroline Louveaux, CIPP/E, CIPM, CPO, Mastercard
Andrea Jelinek, Chair, European Data Protection Board; Head, Austrian Data Protection Authority

This session will give insight into how the European Data Protection Board has laid the foundations for enhanced enforcement cooperation among DPAs, and on the measures it has taken to further intensify this cooperation. You will also get an update on the cases of strategic importance and a preview of what is in the pipeline for the EDPB in the coming months.

What you will learn:
- An update on the DPAs’ enforcement activities.
- Insight into the actions taken by the EDPB to optimise enforcement cooperation, including its work on strategic cases and on cloud in the public sector.
- Information on the EDPB’s strategic priorities for 2023.

(Tags: Traditional Breakout, Enforcement, Policy & Governance)

10:30 – 11:45

[Thursday, 17 November, 10:30 – 11:45]
Closing General Session

Nina Schick, Author of “Deepfakes: The Coming Infopocalypse”

The practical reality of artificial intelligence is evolving into a synthetic future where media is manipulated or even wholly generated by AI. Nina Schick offers insight into how to navigate and understand the exponential technological changes of our age.

12:15 – 13:15

Behavioural Biometrics: A Clash Between Privacy and Security?

Moderator: Lokke Moerel, Senior Of Counsel, Morrison & Foerster; Professor, Global ICT Law, Tilburg University
Stephen Bonner, CIPP/E, CIPM, Executive Director, Regulatory Futures and Innovation, Information Commissioner's Office
Wim Mijs, CEO, European Banking Federation
Wojciech Wiewiórowski, European Data Protection Supervisor

Banks need to implement Strong Customer Authentication (SCA) for access to their online payment solutions. Many have implemented biometric identifiers, such as facial or fingerprint recognition, to ensure SCA. Recently, however, we see banks moving away from static biometric identifiers towards solutions based on behavioural biometrics, such as key stroke patterns, left/right-handedness, use of short cuts (Ctrl+C) and angle the device is held. The behavioural biometric solutions show better prevention of various forms of online fraud. For example, where users are manipulated by fraudsters into logging in with their biometric identifiers and subsequently transfer money, behavioural biometrics solutions flag where users are under instruction or duress. The EU Second Payment Services Directive ("PSD2") facilitates these innovations, as it requires SCA based on a combination of two elements out of: 1. Knowledge (something only the user knows, like a password); 2.
Possession (information only the user has, like a code sent to their mobile device); and 3. Inherence (something only the user has, such as a fingerprint or behavioural biometrics). Static and behavioural biometric solutions are both allowed under PSD2, but also raise privacy issues and are subject to debate. Recently the ICO reviewed behavioural biometric solutions for SCA by banks (at the request of UK Finance and the UK industry group for the financial sector). The ICO considered the use of behavioural biometrics for PSD2 checks allowed under the UK Data Protection Act, as this use can be considered a substantial public interest, when implemented correctly. But when can behavioural metrics be considered ‘implemented correctly’?

**What you will learn:**
- How behavioural biometric solutions work.
- How they different from biological biometrics and the pros and cons.
- The role behavioural biometrics play in the financial industry.
- How behavioural biometrics can be implemented with privacy-by-design.

(Tags: Traditional Breakout, Biometrics, Finance, Identity Management, Infosecurity, Privacy Engineering)

**Emerging US Privacy Laws: Top Tripwires for GDPR-scoped Compliance Programmes**

Julian Flamant, CIPP/E, Privacy and Cybersecurity Associate, Hogan Lovells
Pollyanna Sanderson, Privacy Regulatory Compliance Team Lead, IBM
Sarah Taïeb-Jaskierowicz, Group DPO, UGI Corporation

European privacy legislation has long been the global high watermark to which multinationals scope their data protection compliance programmes. But, as U.S. states such as California, Virginia, Colorado and Utah implement their own baseline privacy rules, companies who operate on both sides of the Atlantic will need to adjust Euro-centric compliance programmes to also satisfy the particularities of American privacy law requirements. Though many of the emerging obligations substantially overlap with GDPR requirements, others have a distinctly American flavor. In practice, compliance programmes must remain adaptable to accommodate nuance and the continual emergence of federal and state regulation. This panel discussion will feature diverse perspectives from in-house compliance practitioners and outside counsel operating on both sides of the Atlantic.

**What you will learn:**
- A list of top ten compliance tripwires to prepare for in the rapidly expanding U.S. privacy law landscape.
- Practical considerations for adapting GDPR compliance programmes to U.S. privacy laws.
- Analysis of highly-active legislative sessions at U.S. state and federal levels, and notes on what else to expect.

(Tags: Traditional Breakout, Consumer Privacy, Employee Privacy, Policy & Governance, Privacy Law, Regulatory Developments)

**Is Effective Age Verification the Gateway to Protecting Children’s Data?**

Moderator: Anna Morgan, Partner, Head of Privacy & Data Protection, Ireland, Bird & Bird
Iain Corby, Executive Director, Age Verification Providers Association; Project Manager, euCONSENT
Michael Murray, Head of Regulatory Strategy, Information Commissioner’s Office
Claire Quinn, CIPP/E, CPO, Head of the Kids Privacy Assured Program, PRIVO

The GDPR has a clear message when it comes to the personal data of children — it deserves specific protection and organisations who process it must implement extra safeguards, since children may be less aware of the risks and their data protection rights. The first step in applying these higher levels of protection is determining who is a child. However, age verification can pose many technical and legal challenges for organisations. New technologies in this area are emerging and some are moving towards a reliance of biometric data. However, regulatory approaches to age verification technologies can vary broadly, particularly concerning the use of children’s biometric data. This panel discussion will explore current regulatory approaches to age verification and its link to GDPR compliance against the backdrop of current and evolving technologies for identifying underage users.

What you will learn:
• Recent developments in the EU/UK data protection regulatory landscape on the use of age verification.
• How these technologies can help organisations meet the higher standards of protection for children’s data.
• The potential GDPR compliance pitfalls that need to be avoided when deploying technical solutions for age verification.

Privacy and Antitrust: Data’s Mom and Dad Just Got Engaged

Aniek Schadd, Legal Advisor to the Hearing Officer, DG Competition, European Commission
Monika Tomczak-Gorlikowska, CIPP/E, CIPT, CPO, Prosus Group
Alex van der Wolk, Global Co-Chair Privacy, Data Security, Partner, Morrison & Foerster

Though privacy laws and concerns have been around for decades now, they have an older sibling: Antitrust. The regulatory framework governing market concentrations has recently shifted its attention to an area that overlaps with privacy: data. In this session we will explore and explain how these two regulatory regimes are converging and at times clashing. What relevancy for the privacy domain follows from the recent German Facebook antitrust case? What does the draft EU Digital Markets Act mean for a company’s collection and handling of personal information? How do global tech giants navigate and use each set of laws to their advantage? What antitrust fundamentals should every privacy professional know, and which conversations will you want and need to have with your antitrust colleagues? This session will be critical for everyone working in a data-driven environment.

What you will learn:
• The fundamental principles of antitrust law as relevant to the privacy profession.
• Recent regulatory antitrust developments relevant to the personal information domain.
• Which questions to ask and which conversations to initiate with antitrust colleagues in your organisation.
12:30 – 13:30

[Thursday, 17 November, 12:30 – 13:30]

Data Marketing and Attitudes to Privacy: What Happens Next?

Moderator: Sachiko Scheuing, CIPP/E, Co-Chairwoman, FEDMA; European Privacy Officer, Acxiom
Christopher Combemale, CEO, Data and Marketing Association
Josh McBain, Consultancy Director, Foresight Factory
Axel Voss, Member, European Parliament

The use of personal information in data-driven marketing provides consumers with the opportunity to live better, consume better and be more sustainable. But the emergence of privacy laws seeks to balance the customer’s right to privacy with the legitimate interests of companies wanting to serve them. This is a reality backed by strong data that most global consumers believe sharing can help industry and organisations respond better to the needs of all parts of a diverse society. This outcome is one of many from our latest Global Attitudes to Privacy study, which our panel will delve deeper into to show the notable decline in levels of online privacy concern, alongside rising public awareness and acceptance of the role data exchange has in the digital ecosystem. Building on these results, we will explore the interconnection between data marketing, consumer trust and privacy regulatory requirements.

What you will learn:

• How organisations can value privacy to increase consumer trust.
• How brands can achieve a harmonised approach to privacy.
• How self-regulation is ideally positioned to address privacy concerns and what regulators can do to make this easier.

[Wednesday, 16 November, 12:30 – 13:30]

GDPR & CCPA — Lessons for the World

Lothar Determann, Partner, Baker McKenzie
Helen Dixon, Commissioner, Data Protection Commission

Data Protection Commissioner for Ireland, Helen Dixon and Lothar Determann, partner at Baker McKenzie in Palo Alto, will examine recent GDPR enforcement trends and case law in the EU compared with developments in the United States and other jurisdictions. Hear their analysis and recommendations for global businesses on a number of topics.

What you will learn:

• Complaint handling and dispute resolution; policies and contract terms.
• Privacy notices; policies, disclosures and supplemental notices.
• Recommendations on data processing and transfer agreements; formats, contents, negotiations and impact assessments.
• Cookies, tracking and do not sell; consent and opt-out management.
13:30 – 14:15

[Thursday, 17 November, 13:30 – 14:15]
UK Data Protection Reform — Good or Bad for DPOs?

Eduardo Ustaran, CIPP/E, Partner, Hogan Lovells

This session will tackle head on the strategic and operational impact of the UK data protection reform for DPOs with EU, UK and global responsibilities. DPOs are facing an increasingly complex compliance challenge in light of the myriad of privacy frameworks around the world. This has strategic implications in terms of what compliance approach to adopt and what to focus on. Come to this session to learn about the evolving operational responsibilities affecting DPOs under the forthcoming UK framework and devise a strategy that works for your organisation.

What you will learn:
- How the DPO responsibilities under the proposed UK framework differ from the EU GDPR
- What strategic implications the new framework has for a DPO with global responsibilities
- Specific operational suggestions to make the DPO job more effective

(Tags: Traditional Breakout, Regulatory Developments)

14:45 – 15:45

[Thursday, 17 November, 14:45 – 15:45]
Cloud Privacy and the European Data Strategy: Synergies and Reciprocal Effects

Pierre Chastanet, Head of Unit - Cloud and Software at DG CNECT, European Commission
Oliver Draf, CPO, Volkswagen AG, Germany
Stephanie Finck, VP, Government Affairs, EMEA, Salesforce
Jörn Wittmann, Managing Director, SCOPE Europe

Today’s data economy is deeply transforming the modus operandi of international value chains, considerably challenging the fostering of competitive, fair and sustainable markets. This unparalleled asset is anchoring overall economic development, dictating the rhythm and capacity of businesses to innovate and grow. Cloud computing stands in the core of this new paradigm as a major driver of digitalisation. Facing this incredibly dynamic environment, designing effective, long-lasting and innovation-friendly regulatory frameworks becomes imperative. Nonetheless, creating such solutions is extremely complex, especially when adding legitimate concerns with data sovereignty and localization to the equation. Against this background, this panel provides an overview of European regulatory developments and their synergies with the data protection landscape. Panellists will then evaluate how the EU Data Strategy shall transform the current scenario as well as how key stakeholders can optimise regulatory implementation while boosting digitalisation and upholding robust privacy standards.

What you will learn:
- A comprehensive overview of the European Digital Strategy and understanding how it addresses major concerns with issues such as data sovereignty and localisation.
How these upcoming regulatory developments can particularly impact the cloud privacy environment.
Finding out how key stakeholders can concretely support the optimisation of the design and implementation of these regulatory endeavors while preserving robust privacy standards.

(Tags: Traditional Breakout, Cloud Computing, Policy & Governance, Privacy Community, Privacy Law, Regulatory Developments)

[Thursday, 17 November, 14:45 – 15:45]
From Compliance to Strategy: Data as a Board Level Issue & Business Opportunity

Vivienne Artz, Senior Data Strategy and Privacy Policy Advisor, Centre for Information Policy Leadership
Bojana Bellamy, CIPP/E, President, Centre for Information Policy Leadership
Keith Enright, CIPP/G, CIPP/US, CPO, Google
Harvey Jang, CIPP/E, CIPP/US, CIPT, VP, CPO, Cisco
Caroline Louveaux, CIPP/E, CIPM, CPO, Mastercard

Our world is transitioning from industrial-based economies to digital-based economies, and data is driving this transformation. One of the core missions of corporate leadership is to ensure oversight and accountability for the organisation as they adapt to these new realities. This must include oversight by the board over all issues related to personal data, which is rapidly achieving recognition as a key capital asset. This session will explore privacy as an increasing board-level issue and as an integral part of Environmental, Social, and Governance (ESG) responsibilities. This session will also articulate why organisations should elevate data-related issues to the highest level of corporate management — corporate boards — rather than taking the current siloed approach. Finally, the session will explore the benefits and opportunities associated with considering data holistically, and further identify key questions for boards to focus on to enable them to upskill and strategise effectively.

What you will learn:
• An understanding of why privacy and data constitutes a board-level issue and an integral part of Environmental, Social and Governance (ESG) investment.
• Insights into relevant skills and arrangements for corporate leadership as it relates to data at the board level.

(Tags: Traditional Breakout, Policy & Governance, Privacy Law, Privacy Operations Management)

[Thursday, 17 November, 14:45 – 15:45]
Global Data Governance: The Impact of Adoption of GDPR-like Laws Globally

Moderator: Aselle Ibraimova, Senior Associate, Reed Smith
Barry Cook, CIPP/E, CIPM, CIPT, Group DPO, Head of Privacy, Data Privacy Analytics
Peter Farrell, Global Privacy Director, Unilever
Simon McDougall, CIPP/E, CIPM, CIPT, Chief Compliance Officer, ZoomInfo

Join us for a discussion on how your global data protection governance may be impacted by the adoption of laws similar to the GDPR in countries globally. Our panel consisting of the former UK regulator and organisations with a global presence will share views and experience on how they are addressing these changes and how it is impacting their work.
This includes taking a look at the increasing number of countries with extraterritorial application of data protection laws, use of data transfers tools, exercising of data subject rights and data breach notifications.

What you will learn:
- A heat map showing countries with GDPR-like laws, data breach notification requirements, data subject rights and DPO requirements.

(Tags: Traditional Breakout, European Union, Policy & Governance, Regulatory Developments, Trans-Border Data Flow, United States)

[Thursday, 17 November, 14:45 – 15:45]
Is the Press the (Best) GDPR Enforcer?

Moderator: Diletta De Cicco, CIPP/E, Associate, Steptoe & Johnson
Luca Bertuzzi, Digital and Media Editor, Euractiv
Vincent Manacourt, Technology Reporter, POLITICO

Privacy is getting more and more attention from sector-specific press; it is even making the headlines of more generalist players. Whether it is to keep privacy pros informed of recent developments and trends in the area or to reach a global audience, the challenges are the same (and not completely new): how to be fast and qualitative and how to balance the need for punch lines with sound thinking.

But there is even more than that: with the perceived lack of effective enforcement of the GDPR, ‘campaigning’ often has much more significant effects than activities of the supervisory authorities themselves. Actual media findings are triggering the launch of investigations. They are also leading to (contentious) processing activities to be stopped ahead of any investigations. What does this tell us about the role of the media? What is our responsibility as a privacy community?

What you will learn:
- A better sense of what drives the generalist and specialist press in the area.
- The challenges they are confronted with (and the consequences this has broadly).
- A better understanding of risks associated with #Iwant2befamous moments.

(Tags: Traditional Breakout, Education, Enforcement, European Union, Privacy Community, Regulatory Developments)

15:00 – 16:00

[Thursday, 17 November, 15:00 – 16:00]
First EU GDPR Certification: Time (& Journey) to Move Forward!

Louis-Marie Guérif, Group DPO, Digital Sobriety Specialist Piano
Alain Herrmann, Commissioner, National Commission for Data Protection of Luxembourg
Fabrice Naftalski, CIPP/E, CIPM, Partner, Attorney at Law, Global Head of Data Protection, EY Société D’Avocats
Sébastien Ziegler, Chairman, European Center for Certification and Privacy

After two years of procedure and following rich interaction with the European Data Protection Board (EDPB) and the Luxembourgish supervisory authority (Commission Nationale de Protection des Données), the EDPB is finalizing the review of Europrivacy to
serve as European Seal under Art. 42. of GDPR, with a decision expected in September. This panel aims to elaborate on the benefits and the operating model toward certification for data controllers and data processors.

**What you will learn:**
- The benefits for applicants of certification vis-à-vis regulators/data protection authorities, judges and markets at large (including public and private donors).
- The process/journey for certification: steps, timeline, deliverables, scope, target of evaluation and contributors.
- The roles/tasks of involved stakeholders: European Centre for Certification and Privacy/Scheme owner, applicant, supporting partners, certification and accreditation bodies.
- The panellists’ first certification journey.

(Tags: Traditional Breakout, Certification, European Union, Policy & Governance, Regulatory Developments)

[Thursday, 17 November, 15:00 – 16:00]
**Smile, You Are on Camera — Face Detection as Audience Measuring Technology**

**Joanna Rozanska, CIPP/E, CIPP/US**, Senior Associate, PricewaterhouseCoopers

Nowadays, technologies capable of detecting, analysing and measuring individuals in public places, such as face detection, have become a reality and the characterising element of the growth and definitive affirmation of a new, global audience measurement market. Although face detection, as opposed to face recognition, is not able to associate the face with a specific person, it does detect the presence of a human face in an image or video and, based on the use of AI, obtains some further information deduced from the features of the face, such as gender, age group or emotions of the viewer. Although the growth prospects for businesses using face detection as audience measuring technology are evident, there are still concerns regarding the impact of this technology on the rights and freedoms of EU citizens and the protection and distribution of personal data.

**What you will learn:**
- How face detection technology can be a powerful tool for business analytics, providing in-depth insights into customers’ profiles and behaviors.
- Major decisions of the European data protection authorities, and how the processing of personal data using physical audience measuring technology is lawful when certain conditions are met.
- In application of the Privacy by Design principle, businesses shall make sure that the technical and organisational measures recommended by the data protection authorities and adjusted to the specific technology used in each case are adopted during the initial design stage of the initiative.

(Tags: Traditional Breakout, Business of Privacy, Consumer Privacy, European Union, Marketing, Privacy Enhancing Technology)

**16:15 – 17:15**

[Thursday, 17 November, 16:15 – 17:15]
**Data Protection Through Ethical AI**
**Ivana Bartoletti**, Global CPO, Wipro; Visiting Policy Fellow, University of Oxford; Founder, Women Leading in AI Network
**Christian Lawaetz**, Chief Technology Officer, Co-Founder, Valuer.ai
**Mikael Munck**, CEO, Founder, 2021.AI
**Tero Ojanpera**, Chairman of the Board, Silo.AI
**Alf Rehn**, Professor of Innovation, Design, and Management, University of Southern Denmark

With the continued adoption of artificial intelligence in solutions across industries and applications, we experience an increase in AI being applied to personal data, with huge potential impact on the data privacy of subjects. Our continuing technological development requires tangible methods and guidelines to ensure the adoption of privacy by design for products and solutions powered by AI. The time is now to discuss and identify how technology and regulation can co-exist and enhance each other to ensure AIs process data subjects ethically and ultimately according to our regulations.

**What you will learn:**
- The current and future predicted adoption of AIs processing personal data.
- The dangers and pitfalls of AI working with personal data.
- The limitations of regulations from the perspective of AI and AI development.
- Why ethics is important when we are talking about regulating AI.
- Solutions, methods and frameworks to develop ethical AI.

(Tags: Traditional Breakout, Ethics, European Union, Policy & Governance, Privacy Opinion, Telecommunications)

[Thursday, 17 November, 16:15 – 17:15]
**How Can We Build a Privacy-aware Commerce Experience?**

**Christel Cao-Delebarre, CIPP/E, CIPM**, Product Privacy Policy Manager, EMEA, Meta
**Kaidi Kikas**, Privacy Policy Manager, Meta
**Daniel Knapp**, Chief Economist, IAB Europe
**Manouk van Dalm**, Marketing Manager, Creative Cosmetics

While upcoming regulations have the overarching goal of benefiting consumers and businesses alike, it is vital that small businesses do not draw the short end of the stick as a result of the significant practical challenges they face in relation to platform changes, which in turn may ultimately hurt their competitiveness and growth. As more customers move online and away from physical stores, businesses are having to adapt to stay in business and data provides a way for businesses of all sizes to continue to reach new customers and accelerate selling goods and services. In this session, experts in commerce and privacy discuss the privacy and policy issues with e-commerce today and in the future; and how to foster privacy-aware commerce experiences that both protect consumers and enable new forms of creativity. Participants will be discussing topics such as social commerce, personalised shopping experiences, monetisation and advertising, consumer protection and the metaverse.

**What you will learn:**
- The challenges of small e-commerce businesses.
- What the future of the e-commerce ecosystem may look like.
- What privacy and policy regulations mean for e-commerce today vs in the future.
- Opportunities platforms such as Meta can provide.
Solving The EU - US ‘Schrems II’ Dilemma: Focus on FISA in Practice & Encryption

Benjamin Baueerle, Head of Data Privacy Legal and Strategies, Siemens AG
Julia Kaufmann, CIPP/E, Partner, Osborne Clarke
Ute Rosenbaum, CIPP/E, Privacy and Cyber Security Expert, Siemens AG
Stephen Vladeck, U.S. Security Law Expert, University of Texas School of Law

With the ruling in the matter of “Schrems II,” controllers and processors have been left questioning the future of transatlantic data flows. In its recommendations 01/2020 the European Data Protection Board discusses two aspects that deserve a closer look: how FISA Sec. 702 is applied in practice and how cryptographic technologies can be utilised. Together with Professor Steve Vladeck, who gave his expert opinion on U.S. surveillance law to the European Court of Justice in the “Schrems II” hearings as well as to the German Datenschutzkonferenz, we will demystify how U.S. surveillance laws work in the context of EU data protection law. Based on that analysis, we will discuss with a cybersecurity expert what type of encryption methods could serve as way out of the data transfer dilemma. Bringing together EU and U.S. legal and cryptography experts, this panel provides a comprehensive picture on various aspects to consider in the context of “Schrems II.”

What you will learn:
- An understanding of how FISA works in practice and which data is relevant when applied in practice.
- A high-level overview of encryption methods and how effective those are in light of FISA practices.

Third-party Risk Management: Improve Cybersecurity Posture & Business Continuity

Rodrigo Cunha, CIPP/E, CIPP/US, Global Director, Digital Ethics, DPO, Anheuser-Busch InBev
Diogo Figueiredo, Global Director, Data Privacy and Digital Risk, Anheuser-Busch InBev
Federica Vons, CIPP/E, CIPT, FIP, Global Legal Director, Direct to Consumer, Anheuser-Busch InBev

With the rapid advancements in cloud, SaaS, PaaS and IaaS technologies and supply chain integration, external vendors are becoming increasingly integrated in fundamental business functions. While the benefits of outsourcing are overwhelming, the engagement of third parties also comes with a risk. After all, while you can delegate authority, you cannot delegate accountability. Vendors become extensions of our internal teams and/or business processes; we are interconnected, and we share data and responsibility for creating a secure ecosystem. Though risk appetites may differ, effective oversight and due diligence are required for corporate success and ethical management of any company. In this presentation we will explain what is at stake — focusing on regulatory and reputational factors. We will also examine key challenges and share what we believe are the indispensable elements of a successful vendor-management programme regardless of
maturity level, from onboarding to effectively evaluating and balancing the risk on an ongoing basis.

**What you will learn:**
- How to effectively onboard internal and external stakeholders, divide the roles and responsibilities, while ensuring that everyone is on the same page in order to increase accountability and commitment.
- Given that protecting internal perimeter is not sufficient anymore to guard business continuity, you will learn about the benefits of connecting the TPRM process—bring together all the different intermediaries to release the value and potential of data.
- How to leverage new technologies and automation to identify the risks as they arise, enable data-driven decisions, and increase both the efficiency and the overall effectiveness of the mitigation process.

(Tags: Traditional Breakout, Business of Privacy, Infosecurity, Privacy Operations Management, Security Operations Management, Vendor Management)

**16:30 – 17:30**

[Thursday, 17 November, 16:30 – 17:30]

*Making Two Out Of One: War Stories from a Global Company Separation*

**Vera Jungkind**, Partner, Hengeler Mueller  
**Michael Kaiser**, Head of Department, Hesse Data Protection Authority  
**Axel Kessler**, Chief DPO, Siemens AG  
**Stefan Plier, CIPP/E, CIPT, FIP**, Corporate DPO, Siemens Energy

When an international corporation spins off a significant portion of its business and lists it on the stock exchange, there will be countless privacy challenges for both companies. DPOs on both sides of the fence must be prepared to solve the major issues that come up. Join us for a front row seat into real-life scenarios and the exciting journey of how DPOs tackled a whole spectrum of topics on a massive, global scale. You will also benefit from the regulator’s perspective on recent transactions, including possibilities to reduce complexity for SMEs.

**What you will learn:**
- An understanding of the various stages of a company separation, or an M&A transaction more generally, and awareness of where a privacy professional’s input is required.
- Typical data-related challenges and practical solutions.
- A holistic view on the topic from inhouse DPOs, external counsel and a supervisory authority representative.

(Tags: Traditional Breakout, Employee Privacy, Enforcement, European Union, Privacy Operations Management)