<table>
<thead>
<tr>
<th>Time</th>
<th>Grande Halle</th>
<th>Area 42 Grand</th>
<th>Petite Halle</th>
<th>La Cave</th>
<th>Area 42 Petit</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.1</td>
<td>Registration</td>
<td>Registration</td>
<td>Registration</td>
<td>Registration</td>
<td>Registration</td>
</tr>
<tr>
<td>3</td>
<td>Welcome and Introduction by Paul De Hert</td>
<td>Welcome and Introduction in Grande Halle</td>
<td>Welcome and Introduction</td>
<td>Welcome and Introduction in Grande Halle</td>
<td>Welcome and Introduction in Grande Halle</td>
</tr>
<tr>
<td>8.45</td>
<td>Title TBC organised by IAPP</td>
<td>Data Protection as Corporate Social Responsibility organised by ECPC</td>
<td>Title TBC organised by Canadian Privacy Commission</td>
<td>A Cybersecurity Incident: Who You Gonna Call? organised by Uni Luxemburg</td>
<td></td>
</tr>
<tr>
<td>10.00</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>8.30</td>
<td>Data protection and high-tech law enforcement – the role of the Law Enforcement Directive organised by FRA</td>
<td>Governance and Regulation of AI from the perspective of autonomy and privacy organised by Campus Fryslân/CF</td>
<td>DPAs in the COVID-19 pandemic organised by CPDP</td>
<td>Regulating AI in health research and innovation organised by University of Vienna</td>
<td></td>
</tr>
<tr>
<td>10.30</td>
<td>Are democratic institutions doing enough to protect democracy, freedom and privacy from the threat of unaccountable private monopoly power? organised by Open Markets Institute</td>
<td>Assessing the impact on fundamental rights in AI applications organised by Politecnico di Torino</td>
<td>Genetic data: a challenge for the EU data protection framework? organised by University of the Basque Country/UPV-EHU</td>
<td>A sand storm or just a breeze? What’s the fuss about sandboxes? organised by Norwegian DPA</td>
<td></td>
</tr>
<tr>
<td>13.00</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
</tr>
<tr>
<td>14.15</td>
<td>AI Act CPDP Political Panel</td>
<td></td>
<td>Secondary use of personal data for (biomedical) research organised by CITIP@KULeuven</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.30</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>16.00</td>
<td>Calibrating the AI Act - is it the right framing to protect personal and fundamental right? organised by Microsoft</td>
<td>GDPR-certification schemes: General vs. specific schemes – how do effective schemes look like? organised by Alexander von Humboldt Institute for Internet and Society</td>
<td>Sharing the digital me– a contextual integrity approach for discussing governance of health and genetic data in Cyberspace organised by Uppsala University</td>
<td>Schrems II: 18 months later: much ado about nothing or a game changer? organised by EDPS</td>
<td>Encoding identities: the case of commercial DNA databases organised by University of Amsterdam</td>
</tr>
<tr>
<td>17.15</td>
<td>Regulation of global data flows: a story of the impossible? organised by EDPS</td>
<td>A critical perspective on the AI Act: threats to fundamental and worker’s rights organised by European Trade Union Institute</td>
<td>Dark Patterns - Manipulation by Design organised by TACD</td>
<td>Digital platforms, the new privacy champions? Between myths and realities organised by Computer Law and Security Review</td>
<td>Effective transparency and control measures (including privacy icons): the example of cookie banners. Where do we stand now? organised by Berlin University of the Arts</td>
</tr>
<tr>
<td>18.30</td>
<td>Cocktail sponsored by EDPS in Le Village</td>
<td></td>
<td>Cocktail sponsored by EDPS in Le Village</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please note that this is a preliminary version of the programme.
<table>
<thead>
<tr>
<th>TIME</th>
<th>GRANDE HALLE AREA 42 GRAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.30</td>
<td>Registration in La Cave</td>
</tr>
<tr>
<td>8.45</td>
<td>Title TBC organised by Google</td>
</tr>
<tr>
<td>10.00</td>
<td>Coffee break</td>
</tr>
<tr>
<td>10.30</td>
<td>Title TBC organised by Apple</td>
</tr>
<tr>
<td>11.45</td>
<td>Leveraging AI: Risks &amp; Innovation in Content Moderation organised by Facebook</td>
</tr>
<tr>
<td>13.00</td>
<td>Lunch</td>
</tr>
<tr>
<td>14.15</td>
<td>Title TBC organised by Mozilla</td>
</tr>
<tr>
<td>15.30</td>
<td>CNIL-Inria Privacy Award, EPIC Champion of Freedom Award</td>
</tr>
<tr>
<td>16.00</td>
<td>Panel TBC</td>
</tr>
<tr>
<td>17.15</td>
<td>Title TBC organised by Interpublic Group</td>
</tr>
<tr>
<td>18.30</td>
<td>Cocktail sponsored in Le Village</td>
</tr>
<tr>
<td>Time</td>
<td>Grande Halle</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
</tr>
<tr>
<td>7:30</td>
<td>Registration</td>
</tr>
<tr>
<td>8:45</td>
<td>Panel TBC</td>
</tr>
<tr>
<td>10:00</td>
<td>Coffee break</td>
</tr>
<tr>
<td>10:30</td>
<td>Title TBC, organised by CDSL</td>
</tr>
<tr>
<td>11:45</td>
<td>Practical Perspectives on International Transfers, organised by CPDP</td>
</tr>
<tr>
<td>13:00</td>
<td>Lunch</td>
</tr>
<tr>
<td>14:15</td>
<td>Will the digital ever be non-binary? The future of trans (data) rights, organised by CPDP</td>
</tr>
<tr>
<td>15:30</td>
<td>Coffee break</td>
</tr>
<tr>
<td>16:00</td>
<td>Trust &amp; transparency in AI: Discussing how to unpack the “black box”, organised by Uber</td>
</tr>
<tr>
<td>17:15</td>
<td>Why privacy matters and the future of data protection law, organised by Washington University</td>
</tr>
<tr>
<td>18:30</td>
<td>Closing Remarks by Paul De Hert and Wojciech Wiewiórowski (EDPS)</td>
</tr>
<tr>
<td>19:00</td>
<td>Cocktail in Le Village</td>
</tr>
</tbody>
</table>
To which extent can the principle of transparency be safeguarded, to make sure that individuals are aware of the use of new technology, and whether this framework adequately ensures fundamental rights.

Building on their professional experience and expertise, invited panellists - academics, policy-makers and law enforcement officers - will provide an opportunity to reflect on the data protection legal framework applying to the use of technologies for law enforcement purposes, and its application to current challenges.

Focusing on the law enforcement directive, this panel will provide an opportunity to reflect on the data protection legal framework applying to the use of technologies for law enforcement purposes, and its application to current challenges. Building on their professional experience and expertise, invited panellists - academics, policy-makers and law enforcement officers - will discuss how the existing data protection legal framework applies to law enforcement with respect to the use of new technology, and whether this framework adequately ensures fundamental rights.

- What short of new technologies are used for policing and what are the main issues and concerns raised?
- What are the specificities and challenges of applying data protection principles in the law enforcement context?
- To which extent can the principle of transparency be safeguarded, to make sure that individuals are aware of the use of technologies for law enforcement purposes, and have access to effective remedies when necessary?
- How are the legitimacy, necessity and proportionality of law enforcement technological tools assessed?
- Are current oversight mechanisms sufficient to protect individual's fundamental rights – and notably the right of access to effective remedies?

11:45 – ARE DEMOCRATIC INSTITUTIONS DOING ENOUGH TO PROTECT DEMOCRACY, FREEDOM AND PRIVACY FROM THE THREAT OF UNACCOUNTABLE PRIVATE MONOPOLY POWER?

In 2022, the European commission will deliver its first evaluation and review of the law enforcement directive (LED). While adopted simultaneously to the general data protection regulation (GDPR), this directive did not – at the time – receive the same level of attention as the GDPR did. However, technology for law enforcement and surveillance purposes is increasingly being used, or considered for use, with limited awareness of its potential impact on individuals’ rights and freedoms. Moreover, the technologies available to law enforcement authorities are continuously diversifying, from predictive policing to the use of drones, facial recognition technologies, or smart cameras. This creates new challenges for law enforcement officers and rights defenders alike.

Focusing on the law enforcement directive, this panel will provide an opportunity to reflect on the data protection legal framework applying to the use of technologies for law enforcement purposes, and its application to current challenges. Building on their professional experience and expertise, invited panellists - academics, policy-makers and law enforcement officers - will discuss how the existing data protection legal framework applies to law enforcement with respect to the use of new technology, and whether this framework adequately ensures fundamental rights.

- What short of new technologies are used for policing and what are the main issues and concerns raised?
- What are the specificities and challenges of applying data protection principles in the law enforcement context?
- To which extent can the principle of transparency be safeguarded, to make sure that individuals are aware of the use of technologies for law enforcement purposes, and have access to effective remedies when necessary?
- How are the legitimacy, necessity and proportionality of law enforcement technological tools assessed?
- Are current oversight mechanisms sufficient to protect individual’s fundamental rights – and notably the right of access to effective remedies?

16:00 – CALIBRATING THE AI ACT – IS IT THE RIGHT FRAMING TO PROTECT PERSONAL AND FUNDAMENTAL RIGHT?

In 2021, the European Commission presented its proposal for a novel regulatory framework for AI. The proposal aims to chart the European path to trustworthy development and deployment of AI-driven products, services and systems. This high-level panel will critically examine whether the foundation and structure of the AI Act - grounded in product safety legislation - can properly address risks to fundamental rights such as the right to human dignity, equality between women and men, freedom of assembly or the general principle of good administration.

- What is the rationale behind the AI acts product safety approach?
- What are the potential benefits and shortcomings of that approach?
- Are there learnings from other legal domains that could be helpful (such as tort law or data protection)?
- Does the approach accommodate the socio-technical challenges of AI systems?
• What is the current state of play of post-GDPR adequacy reviews? As adequacy decisions are a long and time-consuming process, what expectations for facilitating data flows between the EU and the rest of the world can they realistically ful-

• Is there an inherent contradiction between “data sovereignty” and data localisation and the “push for the free flow of data in the digital world”, both of which are simultaneously promoted by the EU in various contexts?

• What multilateral solutions could be envisaged and within what timeframe? What can we learn from other models of regulation of data flows?

CPDP2022 PANELS AT AREA 42 GRAND

08:45 – DATA PROTECTION AS CORPORATE SOCIAL RESPONSIBILITY

Academic ⚪ Business ⚪ Policy ⚪
Organised by European Centre on Privacy and Cybersecurity (ECPC, Maastricht University, (NL)
Moderator Paolo Balboni, ECPC, Maastricht University (NL)
Speakers Sophie Nerbonne, CNIL (FR), Stefano Fratta, EMEA, Sarah Bakir Rabobank (NL), Massimo Marelli, ICRC (IT)

In our data-centric global economy, businesses need to consider privacy and data protection as assets rather than simply compliance obligations. It has already been demonstrated that a strategic and accurate approach to data protection can generate a significant return on investment. With a research project currently running at ECPC Maastricht University, a group of academics, businesses and data protection- and intergovernmental stakeholders, studies ways to trigger virtuous data protection companies between companies by creating an environment that identifies and promotes data protection as an asset to responsibly further their economic targets. This can be accomplished through the development of a new dimension of data protection that goes beyond legal compliance, transforming data protection into a new form of Corporate Social Responsibility. Concrete, measurable and translatable guidance for organizations is being developed in order to answer the following questions:

• What are the fundamental requirements of socially responsible data processing activities?

• How can data protection serve as an asset for a company to responsibly further its economic targets?

• How can companies reconstruct Data Protection into an effective CSR framework?

• What are the benefits for companies that embrace data protection as a CSR?

10:00 - COFFEE BREAK

10:30 – GOVERNANCE AND REGULATION OF AI FROM THE PERSPECTIVE OF AUTONOMY AND PRIVACY

Academic ⚪ Business ⚪ Policy ⚪
Organised by Campus Fryslân (NL)
Moderator Andrej Zwitter, Campus Fryslân (NL)
Speakers Linnet Taylor, Tilburg Law School/It’s-it (NL), Elizabeth Coombs (AU), Catherine Jasserand, KU Leuven (BE), Oskar Gstrein, Campus Fryslân (NL)

The EU is the first ‘global player’ to propose a legal framework for the development and use of AI. The EU AI Act adds another layer of regulation for the governance of data infrastructures, which are also addressed by GDPR and other EU instruments. This panel discusses and considers the impact of this overhauled governance framework. The central question is whether the proposed AI governance framework is capable of comprehensively and effectively addressing concerns around privacy and autonomy which arise during the development and use of AI systems. The speakers share observations on gender and stigmatisation, group autonomy and abnormal justice, as well as security (Facial Recognition and Predictive Policing). These sectoral perspectives open a more holistic discussion on how much governance of AI is desirable/needed and whether the EU approach to AI governance will establish a global benchmark.

• How should AI governance address group interests, group privacy and abnormal justice?

• How can governance mechanisms mitigate automated stigmatisation and discrimination related to gender?

11:00 – ASSESSING THE IMPACT ON FUNDAMENTAL RIGHTS IN AI APPLICATIONS

Academic ⚪ Business ⚪ Policy ⚪
Organised by European Centre on Privacy and Cybersecurity (ECPC, Maastricht University, (NL)
Moderator Anna Buchta (BE)
Speakers David Wright, Trilateral Research (UK), Francesca Fanucci, The Conference of International Non-Governmental Organisations of The Council Of Europe (FR), Emil Lindblad Kernell, Danish Institute for Human Rights (DK), Alessandro Mantelero, Politecnico University of Turin (IT)

Digital innovation has reshaped society, benefiting it, but also raising critical issues. These issues have often been addressed by data protection laws, but recent applications of AI have shown a wider range of potentially affected interests. A broader approach focusing on the impact of AI on fundamental rights and freedoms is therefore emerging. Several provisions in the draft EU regulation on AI and in international and corporate documents push in this direction, but do not outline concrete methodologies for impact assessment. Moreover, existing HRIA models are not easily replicable in the AI context. This is despite the important role of such an assessment in relation to the risk thresholds in regulatory proposals. The panel will discuss how fundamental rights can be effectively put at the heart of AI development, providing concrete solutions for a rights-oriented development of AI.

• Are there different types of artificial intelligence risk assessment and, if so, what are they?

• Who should be entrusted with conducting HRias, when and how?

• What are the key criteria that fundamental rights impact assessments need to fulfil, in order to achieve the intended goals?

• How can HRIA be operationalised in the context of AI by providing measurable thresholds for risk management and human rights due diligence?

13:00 - AI ACT: LAWLESSNESS FOR LAW ENFORCEMENT?

Organised by Privacy Platform (EU)
Moderator TBC
Speakers TBC

The AI Act is intended to regulate the use of artificial intelligence in the EU, and is subject of tense negotiations in the European political arena. Surveillance hawks seize their opportunity and are trying to normalise the use of AI by law enforcement in the fight against crime, without significant limits or oversight. Already now, the police is often illegitimately using AI-driven appliances, such as Clearview. What is necessary to be sufficiently protected against the overuse of AI by the police, so that we do not end up in a de facto surveillance society? How could currently lacking oversight and enforcement of data protection rules be reinforced, while still allowing police forces to do their job? This panel focuses on the use of AI by law enforcement in the context of the currently tensely negotiated AI Act.

14:15 – FUTURE OF AI POLICY

Organised by Center for AI and Digital Policy (USA)
Moderator Merve Hickok, aiethicist.org, (USA)
Speakers Virginia Dignum, Allai (EU), Sarah Chander, EDRI (BE), Larissa Zutter, Center for AI and Digital Policy (CH)

AI policy is moving forward quickly. More than 50 countries have endorsed the OECD AI Principles or the G20 AI Guidelines. 2021 saw the introduction of the EU AI Act, the adoption of UNESCO Recommendation on the Ethics of AI, and the Council of Europe’s outline for an international treaty on AI, based on human rights, democracy, and the rule of law. Also, the U.N. human rights chief called for a moratorium on the use of AI techniques that pose a risk to human rights or fails to comply with international human rights laws. But key questions remain about the prospects for “red lines,” the implementation of policy commitments, and the ongoing problem of bias across AI. Panelists will discuss

• Countries have agreed on the need to prohibit social scoring, but there is still no consensus on the need to prohibit facial
surveillance. What steps are necessary to achieve that goal?
• How does endorsement of principles by countries compare to their practices?
• What are the prospects for the EU AI Act
• Which key AI policy developments should we expect in 2022

15:30 - COFFEE BREAK

16:00 - GDPR-CERTIFICATION SCHEMES: GENERAL VS. SPECIFIC SCHEMES - HOW DO EFFECTIVE SCHEMES LOOK LIKE?
Academic ⚫ Business ⚫ Policy ⚫
Organised by: Alexander Von Humboldt Institute for Internet and Society (DE)
Moderator: Kirsten Bock, Unabhängiges Landeszentrum für Datenschutz Kiel (DE) & European Data Protection Board (EU)
Speakers: Sébastien Ziegler, Europrivacy Certifications (LU/CH), Max Von Grafenstein, Alexander Von Humboldt Institute for Internet and Society (DE), Eric Lachaud (NL)

The EDPB has recently published its Addendum to Guidelines 1/2018 on certification and identifying certification criteria per Articles 42 and 43 GDPR and, on this basis, conducted a public consultation process. One key question has been how a scheme must specify the GDPR-provisions with respect to a predefined processing operation. Promoters of general schemes argue that general schemes are more flexible and cost-saving. To the contrary, promoters of specific schemes argue that specific schemes are actually more cost-saving and, above all, are the only way to effectively increase transparency and an EU-wide consistent application of the GDPR. The proposed panel gives an overview of the certification schemes approved so far by Data Protection Authorities or the EDPB and evaluates them against the regulatory objectives of Articles 42 and 43 GDPR.
• What are the regulatory objectives of Articles 42 and 43 GDPR?
• What are the pros and cons of general and specific certification schemes?
• What schemes have been approved by data protection authorities/EDPB so far?
• How far do these certification schemes meet the regulatory objectives?

17:15 - THE AI ACT AND THE CONTEXT OF EMPLOYMENT
Academic ⚫ Business ⚫ Policy ⚫
Organised by: European Trade Union Institute (EU)
Moderator: Gabriela Zanfr-Fortuna, future of privacy forum, global.
Speakers: Aida Ponce del Castillo, ETUI (EU), Diego Naranjo, EDRI (EU), Paul Nemitz, EC Commission (EU), Simon Hania, Uber (NL)

The EC’s AI Act proposes a regulatory approach to the use of AI systems. It does not address the specificities of employment and the protection of fundamental and workers’ rights. In its current version, it is not designed to deal with the privacy and data protection risks of AI, but to promote the growth of a European AI sector, in line with the EC’s oftentimes stated ambition to make the EU a global AI leader. Civil society actors, MEPs and the EDPB have asked the EC to ban remote biometric identification technologies in public spaces. Others, in particular the labour movement, are concerned about the abuse of surveillance technologies in the workplace. How to balance promoting AI and protecting people’s rights? This and other essential questions such as absence of redress mechanisms, liability, governance - will be addressed in this panel discussion.
• Can the AI Act address the specificity of AI uses in employment, including platform work?
• How to balance promoting AI and protecting people’s rights?
• Can the AI Act clearly ban both mass surveillance and worker surveillance?
• How can GDPR be effectively implemented in the context of employment?
10:45 - GENETIC DATA: A CHALLENGE FOR THE EU DATA PROTECTION FRAMEWORK?

**Academic**: Policy

**Organised by**: Panelfit (EU)

**Moderator**: Ine Van Hoyweghen, University Of Leuven (BE)

**Speakers**: Lisa Diependaele, EU Commission (EU), Dr. Iriko De Miguel, University Of The Basque Country/Upiu-Ehu (ES), Marta Tomassi, University Of Trento (IT), Illaria Colussi. Bmri-Eric (AT)

"The EU data protection legal framework was built around the data subject. Normally, we assume that this is a single person. This is not always the case when we consider health data in general and genetic data in particular. As we all know, there are thousands of diseases that have a genetic component. This component is sometimes inheritable. This means that if we gain access to someone's genetic information, we can also know, or at least suspect, what the genetic endowment of his or her relatives may be. This information is therefore very relevant for all those involved. However, the GDPR is mainly built on the perspective of the individual. This perspective does not work so well with the type of issues that genetic information raise. This panel is compromised to analyse such issues from a multidisciplinary point of view:

- Could we consider that genetic data is personal data of different data subjects (not only the one who provided the biological sample)
- Should other people’s rights prevail against the sample donor’s will not to share the data in some concrete circumstances?
- Are physicians allowed to break confidentiality if circumstances recommend it?
- Does the fact that the sample donor is dead make any difference on this framework?

13:00 - LUNCH

14:15 - SECONDARY USE OF PERSONAL DATA FOR (BIO)MEDICAL RESEARCH

**Organised by**: CITIP/Leuven (BE)

**Moderator**: TBC

**Speakers**: TBC

Scientific research in biomedical sciences is largely based on the availability of data. Due to the limitations of anonymization techniques, these data are often personal data. Biomedical research, for example, relies on the patients’ participation and on the use and reuse of special categories of personal data, such as data concerning health and genomic data. The fight against COVID-19 caused several official bodies, amongst which the European Data Protection Board (EDPB), to emphasise that the General Data Protection Regulation (GDPR) is not intended to hinder the secondary use of special categories of personal data for the purpose of scientific research. However, as evidenced by several recent studies, variation in interpretation of the GDPR and national level legislation linked to its implementation have led to a fragmented approach, which brings uncertainty for biomedical researchers and potentially stifles innovation. An additional level of complexity is fostered by the intricate legal framework applicable to biomedical research. Questions remain as regards to the interplay of the GDPR with the soon to be applicable Clinical Trials Regulation (CTR), to biobanks regulation currently not harmonized in Europe and to the rules for medical devices and in-vitro medical devices. Finally, several future legislative acts - such as the Data Governance Act and the planned regulatory framework for the European Health Data Space - despite their promise to foster the use and reuse of data, could all potentially present novel challenges as regards the protection and use of personal data and the interplay with the already existing legal, regulatory and ethical rules.

- Individual autonomy versus public interest. Is it database ownership that spurs the discussion in the field of (biomedical) research? Are controversies triggered through the debate on patients’ ownership of data?
- When personal data are re-used for scientific research, which safeguards are needed? Do these safeguards depend on the type of controller? Do you consider the same safeguards when the data are sensitive data, e.g., relating to health or genomic data?
- On the interplay of other legal frameworks with the GDPR we ask our speakers to zoom in on one specific framework and discuss the challenges and future considerations. Do such frameworks could include the Clinical Trials Regulation, as well as the proposal for a Data Governance Act, the future European Health Data Space regulation, AI…

15:30 - COFFEE BREAK

16:00 - SHARING THE DIGITAL ME: A CONTEXTUAL INTEGRITY APPROACH FOR DISCUSSING GOVERNANCE OF HEALTH AND GENETIC DATA IN CYBERSPACE

**Academic**: Policy

**Organised by**: Uppsala University (SE)

**Moderator**: Joseph Cannataci

**Speakers**: Deborah, Mascalzoni, Crib, Uppsala University (SE), Heidi Beate, Bentzen, University of Oslo (NO)

The European Health Data Space is a step forward for the effective exploitation of Health Data, moving decisively from the concept of ‘open access’ towards ‘open science’. The strong push in the scientific community towards open science already made health and genetic data in research databases available for (re)use by diverse players but not in all the novel context where data are going to be used. The governance of Health Data in Cyberspace, was scrutinized at different levels from different actors on the theoretical and empirical level. In this panel we will discuss governance directions for the use health-related data, looking at results from preference studies conducted with experts and the general public in 12 EEA countries. Results revealed divergences from the GDPR to be discussed with relevant experts. Those results can enrich the discussion for new approaches to governance of data, further conceptualized, in relation to unintended consequences, protection of fundamental rights and societal acceptability.

- What are the elements to be taken into account to reconceptualize open access and open science (taking people preferences into account)?
- What role plays the contextual integrity framework to think governance further?
- Is data driven research taking the human rights framework into account?
- How can we account for responsible science and human rights approaches?

17:15 - DARK PATTERNS - MANIPULATION BY DESIGN

**Organised by**: TACD (EU/US) with Norway Consumer Council (NO)

**Moderator**: Anna Fielder, Transatlantic Consumer Dialogue (EU/US)

**Speakers**: Finn Myrstad, Norway Consumer Council/Ncc (NO), Karen Melchior Mep, Rebecca Slaughter

Deceptive design practices, or ‘dark patterns’, are used to make consumers take actions against their own interests, to the benefit of companies. Common privacy-invasive dark patterns include hidden default settings that maximize data collection, ambiguous language designed to confuse, and consent flows that push toward certain choices. Such practices are particularly damaging in the context of the surveillance economy, when used by the large platforms to increase their market power. The harms caused by dark patterns are not distributed evenly and have a higher impact on people in vulnerable situations, those with low incomes, children, the elderly, or those with disabilities. Existing policies, such as the GDPR, in the EU or US FTC’s section 5 regulations, are not fully equipped to deal with manipulative design practices at scale. However, legislative initiatives are taking place on both sides of the Atlantic.

- What are the drivers/business objectives of ‘dark patterns’?
- How can dark patterns impact individuals and society generally?
- What policy solutions are needed internationally to deal with such practices?
- Will (and how) AI technologies affect dark patterns in the future?
To what extent is it possible to create direct links between data protection engineering technologies and techniques and data protection engineering approaches, the current practices and discuss existing and emerging challenges. The evolution, development and integration of technical and organizational measures into data processing activities play a big role in the effective and legally compliant functioning of the AML/CFT framework. The Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT) framework entails the collection and exchange of information between customers, obliged entities, Financial Intelligence Units (FIUs) and law enforcement authorities, as well as intelligence services in some cases. Such ex-changes usually encompass personal data, the protection of which needs to be respected. The need to align the AML/CFT requirements with the data protection ones is essential for the effective and legally compliant functioning of the AML/CFT framework.

• Under which conditions is the exchange of data between the various actors allowed?
• What are the rights of the data subjects when their personal data are processed for AML/CFT purposes?
• What safeguards need to be in place for the facilitation of transfers of data from the EU to third countries in the context of AML/CFT activities?
• What are the major data protection concerns that arise regarding the exchange of data in PPPs in the AML/CFT field?

What are the major data protection concerns that arise regarding the exchange of data in PPPs in the AML/CFT field?


Digital platforms are now penetrating almost all aspects of our lives. After having built immense walled gardens without conceiving privacy as a core design value, they are now making bolder privacy claims and implementing privacy enhancing technologies (PETs) in different settings. By way of example, Google and Apple have been developing local differentially private techniques for services such as web browsing and maps or federated learning techniques to reduce the processing of behavioral data for marketing purposes. Google and Apple have also partnered to create an exposure notification system in service of privacy-preserving contact tracing. In this panel, CLSR brings together lawyers, computer scientists and regulators to discuss the benefits and limits of a value-by-design approach and its instrumentalization by digital platforms, which are primarily focused upon strengthening their market and information powers.

• Are digital platforms at the forefront of privacy innovation?
• What do these PETs really achieve?
• How do/could digital platforms use these PETs to strengthen their market position & information power?
• What is the role of a supervisory authority in this context and what could be done to counter-balance excessive centralization of power in the hands of digital platforms?
08:45 - A CYBERSECURITY INCIDENT: WHO YOU GONNA CALL?
Organised by Uni Luxembourg (LU)
Moderators Sandra Schmitz, SNT, Université du Luxembourg (LU), Stefan Schiffner, Westfälische Wilhelms-Universität Münster (DE)
Speakers Corinna Schulze, SAP (DE), Florian Pennings, Microsoft (US), N.N., cert.be (BE), N.N., ENISA (EU)

The Proposal for a revised network and information systems Directive (NIS 2.0 Proposal) encourages Member States to implement a single-entry point for all notifications required under the NIS Directive and also under other Union law such as the GDPR and ePrivacy Directive. This panel discusses the organisational and legal requirements for such a “112” single cyber-security emergency number solution, and whether further harmonization of the various reporting obligations is necessary.

10:00 - COFFEE BREAK

10:30 - REGULATING AI IN HEALTH RESEARCH AND INNOVATION
Academic Business Policy
Organised by Department of Innovation and Digitalisation in Law, University of Vienna (AT)
Moderator Tina Otu Anwana, Department of Innovation and Digitalisation in Law, University of Vienna (AT)
Speakers Max Königseger, MLI Meyerlustenberger Lachenal Froeigh AG (CH), Richard Rak, Department of Legal Studies, University of Bologna (IT), Mariana Rissetto, Department of Innovation and Digitalisation in Law, University of Vienna (AT), Elisabeth Steindl, Platform Governance of digital practices, University of Vienna (AT)

AI systems in healthcare can help diagnose disease, prevent outbreaks, discover treatments, tailor interventions and power Internet of Health Things devices. However, the use of AI raises questions about the proper interpretation, application and interplay of EU regulations in force (GDPR, MDR/IVDR) and new legislative initiatives (AIA, European Health Data Space). The panel will debate critical data protection and AI governance challenges regarding the use of AI in health innovation and research. The speakers will discuss regulatory affairs for AI-enabled medical and “well-being” devices, and the potentials and risks of new technologies in the field of mental health. In addition, the discussion will address anonymization and related risk mitigation measures concerning the use of AI in healthcare, and explore the possible implications of regulating AI in light of the foreseen European Health Data Space.

- What are the regulatory concerns and challenges of using new technologies, such as big data and AI, in mental health?
- What are the implications of the AIA for the integration of AI systems with internet of Health Things devices?
- What are the legal challenges and risks concerning the anonymisation of health data and how to mitigate the risks associated with re-identification?
- Is the interplay between the AIA and the European Health Data Space initiative enough to establish a clear set of rules applicable to AI in health research?

11:45 - A SANDSTORM OR JUST A BREEZE? WHAT’S THE FUSS ABOUT SANDBOXES?
Organised by The Norwegian Data Protection Authority (Datatilsynet) (NO)
Moderator Bojana Bellamy, Centre for Information Policy Leadership (CIPL) (UK/Serbia)
Speakers Kari Laumann, Norwegian Data Protection Authority (NO), Chris Taylor, ICO, (UK), Erlend Andreas Gjære, Secure Practice (NO)

Artificial intelligence (AI) offers enormous potential for better, personalised and more efficient services. At the same time AI is data intensive and often challenges basic privacy principles. Can you have your cake and eat it too? This panel will explore the opportunities and limitations of sandboxes as a tool for fostering innovative and responsible AI solutions. The panelists include both regulators and sandbox participants who will share their experiences from the first data protection sandboxes in Europe. The panel will also discuss the role of sandboxes in the proposed AI Act.

- Are sandboxes the right tool to foster responsible innovation?
- Do sandboxes effectively help AI companies overcome regulatory barriers?
- What are the main learnings from the first round of data protection sandboxes in Europe?
- Will everyone have a sandbox in a few years? Are sandboxes the future when it comes to regulating algorithms?

13:00 - LUNCH

14:15 - THE RETURN OF PRIVACY? ‘SMART VIDEO SURVEILLANCE’ EVALUATING DATA PROTECTION IN THE LIGHT OF PRIVACY AND SURVEILLANCE
Organised by VUB Chair in Surveillance Studies
Moderator Rosamunde van Brakel, University of Tilburg/VUB (NL/BE)
Speakers Ola Svenonius, Swedish Defense College (SE)

In 1995, a US philosopher Jeffrey Reiman warned for the risks to privacy posed by the then novel Intelligent Vehicle Highway System. In the same year in the UK, criminologist Clive Norris raised concerns about algorithmic surveillance in the form of emerging facial recognition and ANPR cameras. Almost thirty years later, that future is now a reality and the world is connected in unprecedented ways facilitated by the ubiquitous proliferation of ‘smart’ surveillance cameras. Efforts to address these concerns side-tracked the discussion to issues of data protection, an outcome at least in theory more easily measureable and enforceable. However, when looking at ‘smart’ video surveillance practices in Europe, it becomes clear that regardless of data protection regulation, these have proliferated also beyond security and crime prevention purposes (often in the context of smart cities) and are becoming normalized. It seems that ‘old-fashioned’ privacy and surveillance concerns have been replaced by narrow data protection compliance. Moreover, societal concerns of surveillance, such as social sorting and changing power relations have become even more pertinent with advancements of Big Data and AI, demanding a broader framework that can incorporate collective and societal harms.

In this regard, The VUB Chair in Surveillance Studies panel aims to discuss privacy and data protection in the context of smart video surveillance by asking the following questions:

- What are the main individual, collective and societal harms of smart video surveillance?
- Does data protection regulation undermine privacy and act as an enabler of smart video surveillance?
- Does the proposed AI regulation address ‘old-fashioned’ privacy and surveillance concerns of smart video surveillance?
- How can privacy and surveillance concerns regain importance in data protection policy?

15:30 - COFFEE BREAK

16:00 - ENCODING IDENTITIES: THE CASE OF COMMERCIAL DNA DATABASES
Academic Business Policy
Organised by University of Amsterdam (NL)
Moderator Alexandra Giannopoulou, Institute for Information Law/ IVIR (NL)
Speakers Amade M’Charek, University of Amsterdam/ UvA (NL), Rossana Ducato, University of Aberdeen (UK), Taner Kuru, University of Tilburg (NL), Ela Jakubowska, EDRi (BE)

This panel aims to enable an interdisciplinary discussion on the legal and normative aspects of digital identities operating on a global scale. We focus on the use of commercial genealogical DNA databanks stemming from –off US-based- private companies for criminal investigations all over the world. Namely, we attend to the convergence between surveillance, forensics and direct to consumer DNA technologies. This case is particularly salient because it lies together the rapid rise, and intensive use of biometric identifiers, the commodification of digital identities, and the use of recreational identity services in criminal investigations. The objective in unravelling this practice of converging technologies and uses, is to problematize digital identities, to examine how they become something else when mobilized for different purposes on a planetary scale, and what the social and legal consequences thereof are.

- What are the legal, social, and institutional environments enabling the production of identities produced through commercial DNA services?
- How are the technologies enabling the creation of these daied genomic profiles altering existing perceptions of citizenship and ‘ultimately’ of identity?
- What are the implications of the convergence of different, formerly geographically, legally, normatively isolated systems, uses, and practices around (digital) identities?

17:00 - CONCLUSION
17:15 - EFFECTIVE TRANSPARENCY AND CONTROL MEASURES (INCLUDING PRIVACY ICONS): THE EXAMPLE OF COOKIE BANNERS. WHERE DO WE STAND NOW?

- **Academic**: Business, Policy
- **Organised by**: Einstein Center Digital Future / Berlin University of the Arts (DE)
- **Moderator**: Birgit Sippel, EU Parliament (EU) the ePrivacy Regulation (EU)
- **Speakers**: Estelle Hary, CNIL (FR), Max von Grafenstein, Einstein Center Digital Future (Berlin University of the Arts) (DE)

Cookie consents with manipulative information and decision architectures are ubiquitous, at least perceived to be. The problem of such so-called dark patterns has long been recognised by regulators, studied by scientists and now also fought by data protection activists. But what are positive examples of particularly successful transparency and control measures? On what methodological basis can these be developed, and their effectiveness tested? And what is the current state of research and development of privacy icons that are considered part of the solution? The panel will provide an overview of examples from (law enforcement) practice and the current state of research as well as possible development paths.

- What are the most recent/prominent examples of good and bad transparency and control measures in practice?
- Which role do privacy icons play in this context?
- Which approaches exist in research to design and test good transparency and control measures?
- What is the regulator’s point of view on this?
The GDPR has been in force for nearly four years, but the challenges of enforcing it set it up to be a paper tiger. The one-stop-shop seems to benefit companies, underdelivering on the GDPR’s promise to give individuals back control of their personal data. NGOs and individuals start to turn to courts to enforce GDPR-conferred rights, including to compensation. Yet, the divergences between national laws of EU countries make cross-border actions challenging. National laws may significantly differ as to the burden of proof, the notions of infringement and damage, causality as well as compensation. With no clear rules determining the applicable law there is a growing risk of fragmentation of individuals’ level of protection.

With data. NGOs and individuals start to turn to courts to enforce GDPR-conferred rights, including to compensation. Yet, the one-stop-shop seems to benefit companies, underdelivering on the GDPR’s promise to give individuals back control of their personal data. NGOs and individuals start to turn to courts to enforce GDPR-conferred rights, including to compensation. Yet, the divergences between national laws of EU countries make cross-border actions challenging. National laws may significantly differ as to the burden of proof, the notions of infringement and damage, causality as well as compensation. With no clear rules determining the applicable law there is a growing risk of fragmentation of individuals’ level of protection.

The upcoming Collective Redress Directive holds a promise to offset some of the existing challenges and facilitate collective actions, yet comes with its own uncertainties.

- Why does the one-stop-shop fail to effectively remedy GDPR cross-border infringements?
- How do national divergences in substantive and procedural laws impact cross-border private actions?
- What are the specific challenges faced by NGOs when bringing cross-border private actions, and what are the recent private actions launched?
- What is the interlink between the Collective Redress Directive and the GDPR, and does it signal the advent of a new era for GDPR enforcement?

10:00 - COFFEE BREAK

10:30 – CONCRETE AND WORKABLE SOLUTIONS TO THE GDPR ENFORCEMENT

Organised by NOVB
Moderator TBC

Speakers
- Nina Herbort, Berlin Supervisory Authority (DE), Sophie in’t Veld, EP (EU), Gwendal Le Grand, EDPB (EU), Max Schrembs, NOVB (EU)

Description: Europe is proud to have the most progressive privacy legislation in the world, however the lack of enforcement leads to legitimate frustration of users and small business. In order to unlock the full potential of the General Data Protection Regulation (GDPR) some of the persisting issues related to its enforcement by Europe’s Supervisory Authorities have to be fixed. The panel is aimed at understanding the underlying issues, as well as identifying concrete and workable solutions with key actors like national data protection authorities and EU institutions.

- What are the persisting issues in the area of the GDPR enforcement?
- Why do they occur?
- What solutions are there?
- What are the respective roles of the EU Supervisory Authorities, EU institutions, and civil society organisations?

11:45 – INTERDISCIPLINARY DATA PROTECTION ENFORCEMENT IN THE DIGITAL ECONOMY

Organised by The European Consumer Organisation/BEUC (BE)
Moderator Ursula Pachl, The European Consumer Organisation/BEUC (BE)

Speakers
- Cecilia Tisell, Swedish Consumer Protection Authority (SE), Isabelle Buscke, vzbv (DE), Hans Micklitz, University of Helsinki (FI)

Description: In its 2010 ruling on data retention, the German Federal Constitutional Court stipulated that the legislature is henceforth obliged to exercise greater restraint when considering new retention obligations or authorizations in view of the totality of the various data collections already in place. From this, the German law processor Alexander Roßnagel derived a government obligation to examine the proportionality of the overall burdens on civil liberties on the basis of an overall consideration of all government surveillance measures (the so-called “surveillance calculus” or “Überwachungs-Gesamtrechnung” in German). According to this interpretation, there is a maximum level of state surveillance that must not be exceeded. For example, once a certain threshold is reached, the legislator would have to exchange one surveillance measure for another, ‘move fast and break things’ has been the motto of some of the biggest tech companies. It can be largely debated what they have actually ‘broken’ but one thing is clear: the lines that separated various areas of law (e.g., competition, consumer protection, data protection) have been broken, or at least blurred. This creates many challenges.

- How can we effectively address practices which may infringe several legal instruments at the same time, in several jurisdictions, under the watch of several authorities? Bad actors seek to exploit the cracks and gaps in our system and often get away with little consequences for their actions. Whereas the gravity of those actions might sometimes seem limited when looking through a single lens, the picture quickly changes when we broaden our perspective. It is time for enforcers to move fast and break things too.

- How are existing EU enforcement structures in various areas cooperating with each other?
- How can we achieve effective interdisciplinary enforcement to tackle systemic issues undermining our rights and freedoms in the digital world?
- Is data protection the area that connects all the dots? What about consumer rights protection or competition?
- What role for private enforcement actions (e.g., via consumer and other civil society organisations) to drive change and ensure an interdisciplinary approach to enforcement?
Data minimisation concerns: can location data collected and shared by mobility service providers effectively be an asset or a liability? How can the upcoming Data Act and EU Mobility Data Space address cities' innovation and sustainability goals, while still ensuring that our data is protected and used ethically?

EU Mobility Data Space, which is one of the ten data spaces proposed by the European Commission. Furthermore, we will discuss how citizens can benefit from mobility data without having to sacrifice their rights and freedoms. In this panel we will dive into the upcoming EU Mobility Data Space, which is one of the ten data spaces proposed by the European Commission. Furthermore, we will explore how the Data Act may tap the potential of horizontal (cross-sector) data sharing, while empowering citizens to make better decisions and protect their privacy.

Sharing mobility data for the common good needs careful assessment because context matters. To what extent can citizens benefit from mobility data without having to sacrifice their rights and freedoms? In this panel we will dive into the upcoming EU Mobility Data Space, which is one of the ten data spaces proposed by the European Commission. Furthermore, we will explore how the Data Act may tap the potential of horizontal (cross-sector) data sharing, while empowering citizens to make better decisions and protect their privacy.

How can the upcoming Data Act and EU Mobility Data Space address cities' innovation and sustainability goals, while still safeguarding citizens' privacy?

Are current frameworks, such as the Mobility Data Sharing Agreement, covering stakeholders' needs for legal certainty when sharing data for the common good?

What are relevant use cases for privacy-preserving bolstered exchanges of data in this space?

How to assess the cross-sharing of mobility data in context?

Data minimisation concerns: can location data collected and shared by mobility service providers effectively be anonymised?

**10:00 - COFFEE BREAK**

**10:30 - THE FUTURE OF THE RIGHT TO ACCESS**

**Organised by** FPF

**Moderator** Kelsey Finch, Future of Privacy Forum (FPF) (US)

**Speakers** Cristina Martinez, European Commission (DG CNECT) (BE), Ine Van Zeelnd, VUB (BE)

The right to access is fundamental in the GDPR. It is a great transparency tool. Lately, many studies have shown how to abuse the right to access to steal data. The issue is not the right to access itself but how it is implemented. We will try to discuss how to fix it at the end of this panel.

- Why is the right to access so important?
- What threatens the right to access?
- Right to access: transparency tool or privacy threat?
- How to fix the right to access?

**11:45 - DATA SOVEREIGNTY AND OTHER EMERGING DATA GOVERNANCE MODELS**

**Organised by** CEU San Palo

Research and best practices in addressing risks in AI systems have significantly progressed over the last years. This panel looks at the most challenging problems and advances in research to support fairness, accountability, transparency and equality in AI. The panel will also examine whether the AI Act’s requirements for trustworthiness will be flexible enough to address these objectives, nuanced enough to tackle the diversity of AI systems and their specific risks as well as the pace of innovation.

- Are the requirements able to tackle the socio-technical challenges of AI systems?
- What are the criteria against which the AI Act’s requirements will be measured?
- Are outcome-based goals an alternative?
- How can AI developers be supported in their fairness work in practice?
- How can stakeholders impacted by AI participate in designing fairer and more responsible AI?

**15:30 - COFFEE BREAK**
The GDPR makes over 70 references to data processing certification in line with its art. 42, including for cross-border data transfers (Art. 46). Similar certification mechanism is embedded in other data protection regulations. This session will provide an overview of the latest developments in data protection certification in Europe and internationally. The session will start by introducing the recent evolution of data protection certification. The Swiss Supervisory Authority (FDPIC) will present the experience and perspective of data protection certification in Switzerland based on many years of experience. The Council of Europe (CoE) will provide a complementary perspective on data protection certification at the international level. The European Centre for Certification and Privacy (ECCP) will present and discuss some innovative models in certifying the compliance of data processing under the GDPR and other regulations. The session will conclude by a panel discussion on expectations, challenges and opportunities with regards to international and mutual recognition of such certification.

- What are the lessons learned and opportunities with data protection certification?
- What is the potential for international recognition of data protection certification?
- What are the differences between universal, specific, and hybrid certification mechanisms? What are their benefits and disadvantages?
- What challenges organisations face following the adoption of the GDPR?
- What are the current state-of-the-art certification solutions for certifying and demonstrating GDPR compliance?

17:15 – DATA PROTECTION AS PRIVILEGE? DIGITALISATION, VULNERABILITY AND DATA SUBJECT RIGHTS

**Organised by** SPECTRE project (BE)  
**Moderator** Jonas Breuer (SPECTRE/VUB)  
**Speakers** Yigid Aydin, European Sex Workers Rights Alliance (EUS), James Farrar, Worker Info Exchange (UK), Gianclaudio Malgieri, LISTS / Vrije Universiteit Brussel (BE), Dr. Paola Pierri, Democratic Society (EU)

Vulnerable individuals and communities are impacted by a lack of digital literacy and e-inclusion in today’s digitalised societies, which idealise the “tech-savvy, independent, and uber-modern, able to produce digital data and analyze it to hold city government accountable” as Burns and Andrucci (2020) argue. This panel revisits vulnerability, zooming in on the impacts of digital technologies. It discusses how new forms of vulnerability are created, or existing ones exacerbated in societies in transition in the digital age such self-expression and participation in civic life and in the digital economy, as well as relationship-building and well-being, to name just a few application areas with policy implications.

- What are vulnerable data subjects, and what is the interplay of new and old vulnerabilities with increasing digitalisation in our society?
- Can data protection law, and especially the data subjects rights, help vulnerable individuals to improve their position in society/ avoid exploitation?
- Have they been used in practice to counter vulnerabilities though, or are they a privilege, mainly at the hands of tech-savvy elites? What other, more collective tools, exist to address digitalisation’s adverse and uneven impacts on certain groups?
- Faced with many problems in the offline world (poverty, literacy, socio-demographic background, inequalities, disenfranchisement and so on), how can vulnerable individuals as well as their representative organisations understand the impacts of digitalisation and act upon them?
More than 155 million people have recovered from Covid-19. However, the symptoms can last longer than expected. Remote patient monitoring with the use of speech and video technologies has proven to be an effective means to monitor the vital signs of frail people as well as healthy individuals who may be at risk of infection. The potential for wearable and wireless sensor technologies to reliably measure physiological parameters and habits of people appears to be great and likely to remain so even in the post-pandemic context.

On the other hand, since healthcare technology is increasingly integrated in private spheres and captures highly sensitive personal data, these developments may cause serious concerns about privacy and data protection. For this reason, a dialogue about the legal and ethical challenges in Active Assisted Living is necessary to develop widespread awareness on these topics.

- What are the ethical, legal, and privacy issues associated with audio- and video-based AAL technologies?
- What is the role of data protection law when it comes to safeguarding sensitive classes of data like race, age and gender collected by audio- and video-based sensors in the home?
- What privacy-by-design methodologies are available in order to protect the fundamental rights of those being monitored by audio- and video-based AAL technologies?
- How can we combine perspectives on privacy and data protection issues arising from the use of AAL technologies concerning healthcare automation?

11:45 – BIG BROTHER OUT TO LUNCH

Organised by PROTEIN (H2020 project) (EU)
Moderator: TBC

Personalized nutrition technologies leverage on the collection and analysis of large volumes of data related to individuals’ dietary behaviour patterns, physical activity and other parameters to provide generic and tailored nutrition, fitness and lifestyle advice. Till today there is no common definition as to what personalized nutrition entails. What there is agreement on is that it is a multifaceted concept of many levels and fragmented regulation. This panel discusses some of the impacts that such technologies have on private life. On one hand, the panel delves onto the concerns about the use of sensitive personal data, the surveillance one subjected to while eating, shopping for food, or doing sports, and the trustworthiness of applications marketed as well-being apps while impinging on health status. On the other, the panel draws attention to the blurred lines between lifestyle and health, health data and non-health data, medical and non-medical context – leading ultimately to questions of consumer safety, discrimination and stigma.

- How has our relationship to food and nutrition evolved over the years, both at an individual and a societal level?
- How ‘personalized’ is personalized nutrition in practice? What are the legal implications when widely available personalized nutrition products are consumed by the non-intended consumer or the non-intended consumer group?
- How does food law interact with data protection law and medical device legislation?

13:00 – LUNCH

14:15 – PRIVACY DESIGN, DARK PATTERNS, AND SPECULATIVE DATA FUTURES

Organised by SnT, University of Luxembourg (LU)
Moderator: Cristina Santos, University of Utrecht (NL)
Speakers: Regis Chatellier, CNIL (FR), Georg Philipp Krog, Signatu (NIO/CH), Stefano Leucci, EDPS (EU), Dusan Pavlovic, Better Collective (SER/DK), Arianne Rossi, SnT, University of Luxembourg (LU)

Opposite forces harshly confront each other on the battlefield of digital services. On one side, privacy-invasive mechanisms like dark patterns pervert the fairness that should govern personal data use. Neither legislation nor slow-paced case law seems able to counteract the pervasiveness and impact of online manipulation.

On the other side, the harm caused by malicious designs is increasingly being exposed and a growing number of transparency-enhancing technologies is being created to support the rights of data subjects.

But we can only devise and implement overarching data protection by design if we become able of anticipating trends, explore the future implications of technology and guide its development towards desirable outcomes. In the end, which bright-era worlds do we intend to design to ensure fair, transparent, human-centred use of personal data?

- How are businesses, academics and regulatory bodies currently mitigating dark patterns?
- What kind of transparency mechanisms should be further designed?
- How might we anticipate emerging trends to prevent risks and drive the development of data-driven services?
- How might law, human-centred design and foresight work together to breed trust in digital services and fight online manipulation?
their disapproval of, but introducing legislation to prevent their use and have even brought enforcement proceedings against major technology platforms accused of using dark patterns. This panel aims to discuss the role of consumer protection, in particular the Unfair Commercial Practices Directive and consumer protection enforcement for protecting users from all forms of data driven manipulation.

- Can consumer protection regulation mitigate the shortcomings of data protection law in dealing with dark patterns and data-driven manipulation?
- How can using evidence-led insights into how dark patterns manipulate behavior inform policy and rule makers?
- How will changes to the Unfair Commercial Practices Directive provide protection from dark patterns and data driven manipulation?
- Can consumer protection bridge the enforcement gap?

17:15 – TECHNOLOGY AND POWER IN TIMES OF CRISIS

Academic ★★★ Business ★ Policy ★★★
Organised by Global Data Justice project, Tilburg University (NL)
Moderator Linnet Taylor, TILT (NL)
Speakers Christian D’Cunha, DG Connect (BE), Mariana Rielli, Data Privacy (BR), Grace Mutung’u, CIPIT (KE)

This panel will examine how new markets and opportunities opened up by the Covid-19 pandemic have shaped business strategies for technology firms in the EU and worldwide. Technology firms are increasing their markets in public health logistics (contact tracing, vaccine certification, information distribution), educational technology and many other areas thanks to the pandemic. Less visibly, there is huge growth in the market for ID and biometric technologies, bordering technologies and home-working surveillance applications. These shifts have been accompanied by decreased controls on competition and an increased tendency on the part of authorities to legitimise pandemic-related innovation even when it challenges established boundaries. The panel will discuss the implications of these power shifts for regulators and advocacy organisations, comparing different regional challenges and possible policy and regulatory responses in the areas of privacy, data protection, competition regulation and civil society action.

- How has the emergency of the pandemic reshaped markets for technology firms?
- What new challenges does the pandemic create for policymakers, regulators and advocacy organisations interested in digital justice and rights?
- Do pandemic-related shifts in technological power differ across regions?
- How should regulatory and civil society power balance these shifts in market share and commercial infrastructure?
17:15 – WHY PRIVACY MATTERS AND THE FUTURE OF DATA PROTECTION LAW

Organised by Cordell Institute @ Washington University (USA)

Moderator Helen X. Dixon (IR)

Speakers Frederik Zuiderveen Borgesius, Radboud University (NL), Natali Helberger, University of Amsterdam (NL), Mireille Hildebrandt, VUB (BE), Neil Richards, Washington University (USA)

Data protection laws are currently spreading across the globe, but they are often proposed and enacted without much consideration of their definitions of privacy and the human values that they support. A complete consideration of “data protection and privacy in transitional times” requires us to reconsider why privacy and data protection rules exist, what values they serve, and what they should look like in the future. This panel brings together European and American academic and regulatory experts to ask these hard and essential questions of privacy and data protection law. Using the argument in Neil Richards’ recently published Why Privacy Matters (OUP 2022) as an initial starting point, the panel (and audience) will discuss the big questions of what privacy and data protection law is, what it is trying to achieve, and where it falls short.

- Why do privacy and data protection matter? What values do they serve?
- What is the relationship between privacy and data protection rules and identity formation, political freedom, and consumer protection?
- How should our understandings of privacy and data protection change as we confront new problems like public health emergencies, artificial intelligence, and pervasive data collection and computing?
- Is a shared understanding of what privacy is and why it matters possible across the different legal systems on both sides of the Atlantic?

18:30 – CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIÓROWSKI (EPDS)
Today’s data infrastructures, operated and controlled by dominant tech platforms, block the way for more sustainable, privacy-protective and user-centric business models that are accountable towards individual users and mindful of the social impacts. The panel will discuss what regulatory, technological and institutional transformations are needed in order to reclaim the power over data and algorithms from dominant platforms to serve individual and societal goals. Invited experts will discuss the most promising avenues, which include counter-power measures that de-centre tech, new types of infrastructure and new institutions that could emerge.

The panel will acknowledge risks and practical difficulties that come with transformations such as decentralisation or functional separation of dominant platforms via interoperability measures and introducing non-commercial data intermediaries (such as 'BBC for data'). These insights will be based on preliminary findings made by the Rethinking Data working group set up by the Ada Lovelace Institute.

- How are measures proposed in draft DMA/DSA/DGA regulations addressing the lack of dominant platforms’ accountability when it comes to their power over data and algorithms?
- Assuming that open, interoperable ecosystems replace closed ecosystems operated and controlled by dominant platforms, what data protection and data security safeguards need to be in place in order to ensure accountability of new institutions (e.g. data trusts or public interest corporations)?
- Under which conditions, including strict data protection and data security requirements, new competitors should have access to open ecosystems, including access to aggregate personal data and ML models (so far controlled by dominant platforms)?
- What might help ‘open the gates’ for new types of data intermediaries and their use of data for social benefit, beyond what has already been proposed in the DMA/DSA/DGA?

13:00 - LUNCH

14:15 - IS A EUROPEAN DATA STRATEGY WITHOUT TRADE-OFFS BETWEEN ECONOMIC EFFICIENCY AND FUNDAMENTAL RIGHTS PROTECTION POSSIBLE?

Academic Business Policy
Organised by Open Future Foundation (NL)
Moderator Balázs Bodo (IVIR, NL)
Speakers Heleen Janssen IVIR (NL) and Computer Science & Technology, University of Cambridge (EN), Alek Tarkowski, Open Future Foundation (NL)

European data strategy and its key legislative measures, the Data Governance Act and the Data Act, have two stated goals. First, the strategy seeks to grow the data economy, innovation and data use in the Single Market. Second, a citizen-centric commitment to European values is declared. These are potentially conflicting goals, as human rights protection is often seen as a barrier to economic growth. EU’s strategy introduces novel data governance models, including data cooperatives, enabling European data policies that support democratic, citizen-centric data governance. Meanwhile, these new governance models might expose participants involved in them to new risks, including the risk of their data being used against them.

- Which policy measures in the new Data Strategy have greatest transformative potential for the Internal Market?
- What are the greatest expected drivers and obstacles of data-driven innovation within the European data strategy?
- What are the potential points of conflict between economic growth from data and fundamental rights within the European data governance framework?
- Can the European commitment to citizen-centric, democratic data governance be maintained under the perceived competitive pressure with China and the US?

15:30 - COFFEE BREAK

16:00 - LIMITS OF EMERGENCY POWERS: PROTECTING PRIVACY IN EXCEPTIONAL CIRCUMSTANCES

Academic Business Policy
Organised by EPIC (US)
Moderator Calli Schroeder, EPIC (US)

The COVID-19 crisis has highlighted the need for strong data protection standards during public health emergencies. Governments and private entities have used contact tracing technologies, employee monitoring, surveillance drones, facial recognition, and more in an attempt to confront the COVID pandemic, justified by a “state of emergency.” Italy, for example, approved the use of drones to surveil lockdown-violators during the pandemic, identify infected individuals, and even yell at offenders through recorded warnings. Under many global legal regimes, certain rights may be curtailed or temporarily limited during states of emergency, exceptional circumstances, or due to pressing national interest. However, privacy advocates have been vocal about the need to ensure that emergency measures are limited – both in time and scope – and not permanently undermine individual privacy rights.

- What limitations – both in law and in practice – currently exist on curtailing privacy protections during a state of emergency?
- How are privacy protections safeguarded by data protection authorities, civil rights groups, and others during a declared state of emergency?
- Are there areas that you believe most urgently require protections against exploitation during a state of emergency?
- How can we effectively combat potential abuse of “state of emergency” to curtail privacy rights?

17:15 - WHEN PRIVACY AND DATA PROTECTION RULES, WHAT AND WHO LOSES OUT?

Academic Business Policy
Organised by The Interdisciplinary Hub for Security, Privacy and Data Governance, Radboud University Nijmegen (iHub) (NL)
Moderator Tamar Sharon, iHub, Radboud University Nijmegen (NL)
Speakers Lee Bygrave, University of Oslo (DK), Augustin Reyna, BEUC (umbrella group for independent consumer organisations in Europe) (EU), Gloria González Fuster, Vrije Universiteit Brussel (BE), Natali Helberger, Institute for Information Law, University of Amsterdam (NL)

When it comes to digital harms, privacy and data protection concerns have come to dominate public debate and regulation. While useful early on in the strike against the new power asymmetries of the digital era, the focus on privacy and data protection is currently engendering detrimental effects. Amongst others, the hegemony of the value of privacy may crowd out other values that are no less important or at risk in digital society – such as solidarity, democratic control and justice – or narrowly redefine them as privacy concerns. The focus on data protection may also be counterproductive at a time when Big Tech is developing privacy-friendly ways to expand into new sectors of society. Moreover, governments may increasingly use privacy to evade discussion and critique. The panel will address the effects of the rise to dominance of privacy and data protection concerns.

- What kind of strategic uses is privacy being put to, by corporations and governments?
- When does data protection law fall short in protecting people from digital harms?
- Which values and rights have suffered from the focus on privacy and data protection, and deserve more attention?
- How can we explain the historical rise to dominance of privacy and data protection in public debate and regulation?

18:30 - CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIÓROWSKI (EPDS)

in Grande Halle
the Digital Single Market are new, strong and robust data protection rules, designed to strengthen the protection of fundamental rights of individuals in the Digital Age. These competing legislative developments are often implemented without objective evidence, which would justify their raison d’être. This panel should therefore explore whether we can empirically measure the use and frequency of digital investigation powers, and, based on such measurements, learn something about their fundamental rights compliance.

• What can we learn from the criminal justice statistics?
• Can we objectify the debate about the necessity and proportionality of digital investigation powers?
• Can we quantify the necessity test? What about proportionality?
• How do we ensure the tracing of the entire life cycle of personal data in the criminal justice system, from the moment of its collection/access until the end of the investigation/trial/sentencing?

11:45 – BOOK SESSION: ‘INDUSTRY UNBOUND’ BY ARI WALDMAN

In his book ‘Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power’, Ari Waldman shows how tech companies undermine privacy protections in practice. Building on years of research and interviews with privacy lawyers and professionals, his book reveals the layers of the tech industry’s stranglehold over privacy regulation. By dominating discourse, compliance, and design, the tech industry has managed to stack the cards against us and so effectively co-opt the privacy profession that even those who call themselves privacy advocates on the inside do not realize how they are complicit in oppressive data extraction. In this special CPDP session, the author will provide an introduction to his book, and engage in a discussion with leading experts about the lessons and insights they draw from this insightful contribution to the field.

• What are the mechanisms through which corporate interests can dominate privacy work?
• What is the relevance of discourse and are there differences between Europe and the U.S. in this regard?
• Do we need more evidence in relation to privacy practices in Europe and the GDPR?
• In what way can privacy practices be made more meaningful in protecting privacy?

13:00 – LUNCH

14:15 – TITLE TBC

Organised by EDEN

15:30 - COFFEE BREAK

16:00 – JUSTICE 3.0: AI IN AND FOR JUSTICE AND CASE-LAW AS BIG DATA CHALLENGES TO ASSIST JUSTICE, PREDICTING IT WHILE PRESERVING FUNDAMENTAL RIGHTS AND FREEDOMS

Both the European regulatory landscape and international markets for legal services display a flourishing of initiatives to expand the use of AI and discovery knowledge. A number of products is the markets while they are outlawed in some countries. Against a backdrop of EU initiatives to foster the re-use of judicial data, the proposed AI regulation shows high suspiciousness on the use of AI in administering justice and in law enforcement while remains rather silent on the use of the same technologies by private entities. Many of the concerns raised by the EU Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe in 2018 still remain largely unaddressed while judicial data as such begins to be seen as a source of social data for policy analysis with KDD and AI methods and tools.

• explore the suitability of the various technologies to preserve adequate levels of personal data protection and bias prevention without losing effectiveness
• test the state of art in data and argument mining from judicial data also for policy;
• consider the ethical constraints needed to steer AI in and for justice
• provide an overview of the possible challenges emerging from considering case law and legal materials as big, possibly open, data

17:15 – TITLE TBC

Organised by BRICS

18:30 – CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIROWSKI (EPDS)
in Grande Halle
8:45 - PERSONAL DATA IN TEXTS: DETECTION, ANNOTATION AND GOVERNANCE

Academic Business Policy
Organised by Université de Bourgogne Franche-Comté (UBFC) (FR)
Moderator Dr Iana Atanassova, Université de Bourgogne Franche-Comté (UBFC) (FR)
Speakers Thierry Bregnard, Haute École de Gestion Arc (HEG-Arc) (CH), Walid El Abed, Global Data Excellence (CH), Sylviane Cardery, Université de Bourgogne Franche-Comté (UBFC) (FR), Hitoshi Ishihara, Otemon Gakuin University (JP)

The new GDPR regulation requires that any company must be able to prove that the personal data it holds are protected and, above all, unusable in case of theft. This has created a new need for automatic tools to identify and mask protected data, including in texts, in order to facilitate companies’ compliance with the legislation. The creation of such tools, that allow robust and versatile text processing to handle personal data, is still an important issue and requires the creation of specific semantic models for linguistic AI.

This panel will outline the current landscape in the processing of personal data in texts, by providing the point of view of both researchers in Natural Language Processing (NLP) and actors of the private sector. It will also address the question of data governance related to personal data in texts.

- What are the real needs of business when it comes to personal data processing for GDPR compliance?
- What is the role of personal data governance for the creation of value?
- How to create linguistic models for the processing of personal data?
- What algorithms do we need for the efficient processing of personal data in texts?

10:30 - PIMS BUILDING THE NEXT GENERATION PERSONAL DATA PLATFORMS, A HUMAN CENTRIC APPROACH

Organised by Internet Users Association
Moderator Marco Mella, Politecnico di Torino (IT)
Speakers Leonardo Cervera-Navas, European Data Protection Supervisor (EU), Rodrigo Irizarzabal, WIBSON CEO, Vili Vilkuna, KU LEUVEN (BE), Nikolaos Laoutaris, IMDEA (ES)

The Personal Information Management Systems (PIMS) concept offers a new approach in which individuals are the “holders” of their own personal information. PIMS allow individuals to manage their personal data in secure, local or online storage systems and share them when and with whom they choose. Individuals would be able to decide what services can use their data, and what third parties can share them.

This allows for a human-centric approach to personal data and to new business models, protecting against unlawful tracking and profiling techniques that aim at circumventing key data protection principles. PIMS promise to offer not only a new technical architecture and organization for data management, but also trust frameworks and, as a result, alternative business models for collecting and processing personal data, in a manner more respectful of European data protection law.

This panel will address PIMS from the perspective of the EU regulatory framework, new business models, tools for implementation and success stories. It will be of special interest for companies, developers and entrepreneurs interested in business proposals based on personal data of European citizens.

11:45 - TRANSITIONAL (LEGAL) TIMES FOR R&D AND R&E SECTORS

Academic Business Policy
Organised by VALKYRIES H2020 Project - LIDER Lab Scuola Sant’Anna - Ethical Legal Unit - (IT)
Moderator Denise Amram, Scuola Superiore Sant’Anna, SSSA, Pisa (IT)
Speakers Rowena Rodrigues, Trilateral Research (UK), Andrea Parziale, EURAC Research Italy (IT), Albena KUYUM-DZHIEVA, Policy Adviser EISMEA (BE), Pedro Ramon Y Cajal, INDRAD (ES)

R&D and R&E sectors are currently affected by the European Strategy of Data as well as by the entering into application of the EU legislative initiatives (Clinical Trials and Medical Device Regulations) and their balance with the ongoing debate on AI Regulation.

The panel explores how the standardization and compliance processes shall deal with the challenges and new obligations emerging by the uncertainties of the applicable ethical-legal framework in order to understand the possible domino effect produced by the GDPR towards the following EU initiatives aiming to enhance fundamental rights in the new technologies.

Specific scenarios, investigated under the H2020 - VALKYRIES project as well (GA 101020676), will be discussed by the speakers, such as the development of AI solutions for first aid and multi-victim disasters, where health-related data are processed.

- Which are the most significant obligations for R&D and R&E emerging from the EU Strategy of Data framework and the already approved CTR, MDR, GDPR?
- What are the challenges in terms of standardization and compliance?
- How the proposal of AI Regulation will impact on the development of solutions?
- Which specific safeguards shall be implemented in case of solutions processing health-related data for emergencies management?

13:00 - LUNCH

14:15 - ROLE OF ETHIC COMMITTEES IN THE EUROPEAN HEALTH DATA SPACE

Academic Business Policy
Organised by CPME – Standing Committee of European Doctors (BE)
Moderator Sjaak Nouwet, KNMG (NL)
Speakers Anvika Eberstein, COCIR (BE); European Commission, DG SANTE (EU); EDPS (EU) tbc; Health Data Hub (FR) tbc; Otmar Kloiber, WMA (INT)

The European Commission is expected to adopt a proposal for a Regulation on the European Health Data Space (EHDS) in the first quarter of 2022. Personal data collected from primary care via the electronic health records could be linked to the EHDS system in order to be used for health research purposes and policy-making. This repurposing activity will be based on the data subject’s consent but might also be based on other legal basis, such as the performance of a task carried out in the public interest or a specific Union law concerning the further processing as compatible and lawful. When consent is not the legal basis, and data are identifiable, the EHDS should foresee greater involvement of ethics committees. This panel will take a deep dive on what specific countries are doing in this area and discuss possible recommendations on how, where and when in the procedure ethics committees could be involved in the EHDS (e.g. one-stop-shop).

- How will the European Health Data Space link clinical data and public health data to support health research and policy decision-making?
- What should be the legal basis for further processing of special categories of health data for health research and policy decision-making?
- What role for ethics committees in the future proposal for a regulation on the EHDS?
- What possible recommendations can be provided?

15:30 - COFFEE BREAK

16:00 - EMPOWERING THE AI ACT: LIMITS AND OPPORTUNITIES

Academic Business Policy
Organised by Smart Global Governance / EDHEC Augmented Law Institute (FR)
Moderator Gianclaudio Malgeri, EDHEC Augmented Law Institute (FR)
Speakers Oliver Guillot, Smart Global Governance (FR)

The AI Act is an innovative innovation in the EU legal scenario. However, both the blacklist and the “high risk” list of AI practices might appear too narrow (the EDPB denounced the lack of protection for biometric identification and emotion recognition) and not flexible enough for the challenges ahead. This panel aims to address, thus, the current limits but also the opportunities of the AI Act proposal. Possible tools could help to empower the current proposal, e.g.: a more flexible notion
of risk, a better consideration of emotion recognition, but also individual rights, including an ex-ante duty of participatory design and development of the AI systems.

- Should the black list in the AI Act include also other AI practices (e.g., emotion recognition, commercial manipulation)?
- Should other tools protect individuals too (e.g. participatory design)? How?
- Is the proposed system of “high risk” classification effective, forward-looking and flexible enough?
- Is the AIA well connected to other existing legal frameworks (GDPR, EU Consumer protection law)?

17:15 – SYNTHETIC DATA MEET THE GDPR: OPPORTUNITIES AND CHALLENGES FOR SCIENTIFIC RESEARCH AND AI

Academic Business Policy
Organised by University of Turin, UNITO, Turin (IT)
Moderator Eleonora Bassi, Senior Research Fellow, Nexa Center for Internet and Society, The Polytechnic University of Turin (IT)
Speakers Theresa Stadler, SPRING Lab at EPFL (CH), Massimo Attoresi, Unit “Technology and Privacy” at EDPS (BE), Pompeu Casanovas, La Trobe University Law School (AU), Jerome Bellegarda, Apple Inc. (USA)

Huge amounts of personal data are increasingly collected by governments and the private sector. Such data are potentially highly valuable for scientists, e.g. work on precision medicine and digital health. Striking a balance between free availability of data for research purposes and the protection of individuals from potentially harmful disclosure and misuse of information, however, is not an easy task. Efforts to guarantee effective de-identification methods have been so far inconclusive, particularly in the context of large datasets where it is extremely difficult to prevent re-identification of individuals. Synthetic data can capture as many of the complexities of the original dataset, such as distributions, non-linear relationships, and noise, and yet, such datasets do not actually include any personal data. We may provide solutions for well understood domains, augment domain data when acquiring such data is sensitive or expensive, and explore machine learning algorithms and solutions when actual domain data is not available. A number of opportunities and challenges follow as a result in the fields of artificial intelligence, e.g. machine learning applications, and personal data processing for scientific purposes, e.g. the re-use of personal data.

- How do synthetic data improve today’s state-of-the-art in AI?
- How can synthetic data improve today’s legal regulations on the processing of personal data for scientific purposes?
- What are the limits, e.g. translational or operative boundaries, of this approach?
- What personal data applications could be a game-changer through the use of synthetic data?

18:30 – CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIÓROWSKI (EPDS)
in Grande Halle