

Data Protection Insider

Issue 19, 19 March 2020

- The CJEU and Consent Procedures: Opt-Out as Consent? -

On 4th March 2020, Advocate General Szpunar delivered his Opinion in the case of *Orange Romania*. The referring court had asked whether individuals who intend to enter into a contract with a telecommunication services provider – Orange Romania *in casu* – can have given their freely given, informed and specific consent if they were required to make a handwritten statement that they do not consent to Orange Romania photocopying and storing their identity documents. Advocate General Szpunar submitted that consent is not freely given if the customer has to declare in writing that he does not consent. To support his argument, the AG referred to the recent *Planet49* judgment in which the CJEU found that having to untick a box in order to refuse to consent to processing runs contrary to the GDPR – which requires a positive action by the data subject to consent to processing. Furthermore, according to Szpunar, the approach taken to securing consent, *in casu*, cannot be regarded informed because the customer does not know that he is not obliged to consent to the photocopying of his ID in order to conclude the contract. In addition, the AG deemed that requiring a customer to consent to the copying and storing of ID data is beyond what is necessary for the performance of a contract under Article 6 (1) (b) GDPR. Finally, the AG submitted that it should be for the controller to demonstrate that the customers have consented to the processing of their data, instead of documenting that some have refused. The case demonstrates that the legal details of consent remain a subject of debate whilst the practical implementation of consent remains problematic. The case is likely to leave data protection experts scratching their heads. How is it possible that opt-out is still being discussed as a legitimate approach to obtaining consent? Even more perplexingly, how and why does such a case – giving the clarity of the legal situation – need to be referred to the CJEU?

[Learn more](#)



- UN Special Rapporteur on Privacy's Recommendations on Gender -

The UN Special Rapporteur on the Right to Privacy has produced a set of Recommendations dealing with the Right to Privacy and Gender. The need for the Recommendations emerged on the back of the finding, over the course of the Rapporteur's work, of 'deeply disturbing breaches of privacy relating to individuals' gender'. In terms of scope, the Recommendations are designed to function as a practical guide in relation to both state and non-state actors and to provide a set of framework principles for the protection of 'the privacy of all individuals, inclusive of binary female and male, and individuals of diverse sexual orientation, gender identity, gender expression and sex characteristics'. In terms of content, the Recommendations deal with a broad spectrum of issues raised by the intersection of privacy and gender. These include – amongst many others: asylum seeking, healthcare, physical and reproductive autonomy, civic and cultural activities and gender identity. The work of the Special Rapporteur in putting together the Recommendations is – as always – impressive. As far as we are aware, this is the most comprehensive set of Recommendations dealing with Privacy and Gender currently available. In this regard, even if the Recommendations are not themselves hard law, they should nevertheless be considered an instrument with significant hortatory power. In this respect, they provide a framework on which future national and international instruments might build.

[Learn more](#)



- EDPB Statement on Data Protection and Covid -

On 16th March, Andrea Jelenik, the Chair of the EDPB, released a statement on the processing of personal data in the context of the Covid outbreak. She stated: 'Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data.' The statement itself is not extensive, controversial or problematic. The statement is interesting, however, in highlighting the significance of the Covid outbreak for data protection law. The details of data protection rules in relation to emergency situations such as the Covid outbreak are only vaguely defined in the GDPR. Accordingly, national and European DPAs will be in the front line of providing the necessary concrete clarifications. How these organisations choose to set the balance data protection principles and the public interest has the potential to significantly shape future data protection discussions. Two shaping functions deserve mention. First, rules set in the context of Covid will be integrated into data protection jurisprudence and will continue to alter the legal landscape long after the outbreak has subsided. Second, and more importantly, rules set in the context of Covid have the potential to drastically shape public perception of the social function and utility of data protection law. Personal data will be a hugely valuable asset for governments and organisations setting plans in relation to Covid. How rules on the processing of personal data relate to these activities will thus be a matter of significant public interest. Will DPAs strike the right balance, and successfully portray data protection law as a flexible and reasonable framework for the balance of rights and interests in information? Or will DPAs insist on technically correct, but contextually blind, interpretations of data protection law, and succeed only in portraying data protection as an unnecessary obstruction to legitimate social activity?

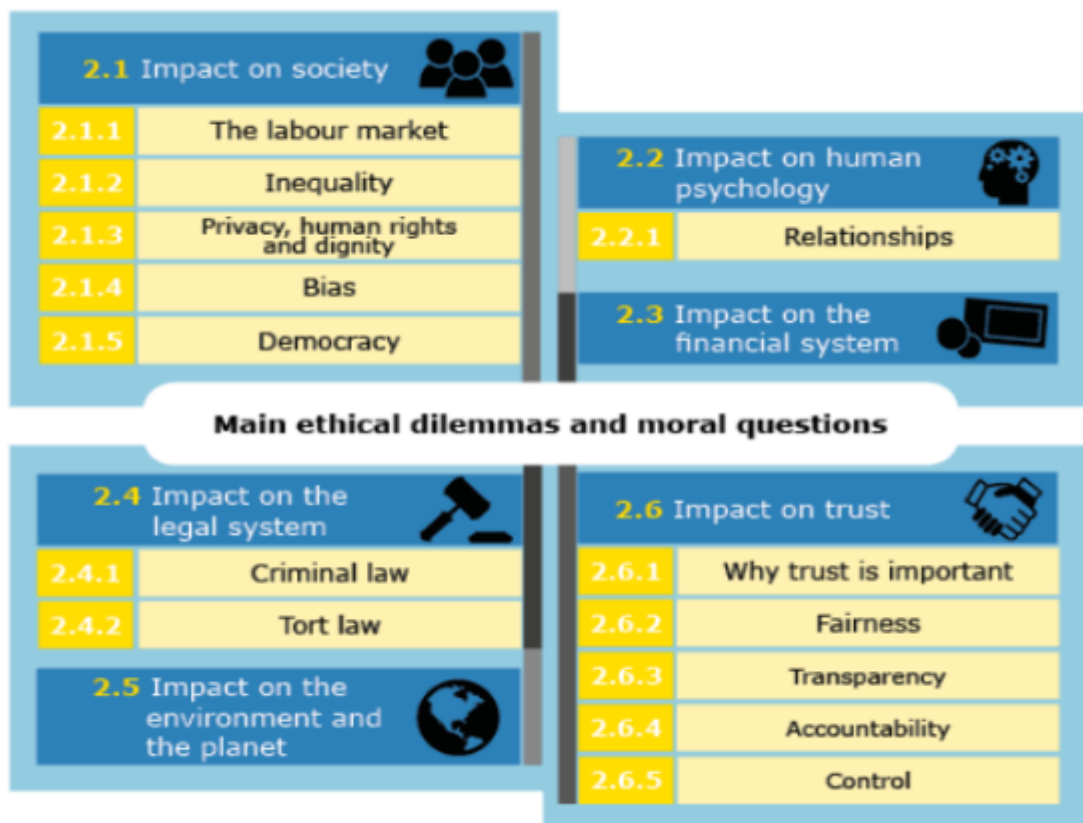
[Learn more](#)



- Study Finds Only 10% of SMEs are GDPR-compliant -

A study by the UK Data & Marketing Association (DMA) has found that only 10% of SMEs are *fully* compliant with the GDPR. Only 65% are rated as being halfway, or three-quarters of the way, to compliance. However, the same study found that over 60% of the companies believed themselves to have a moderate-to-good understanding of the GDPR and that over 70% deemed their company to have a high understanding of the GDPR. The figures are surprising: 70% of the companies surveyed deemed themselves to have high knowledge of the GDPR, whereas only 10% seem to have implemented this knowledge in practice. This raises questions as to where the problem in compliance lies. Does the problem lie in the lack of knowledge, the lack of training opportunities for SMEs, in the lack of motivation to comply or in some other issue? According to Tim Bond, head of insight for DMA, the problem is both lack of knowledge and training. For example, he points out that 38% of SMEs seem to believe that the GDPR does not apply to customer data. This assertion simply raises further questions: is the purported lack of training and knowledge due to lack of resources – i.e. is the GDPR too burdensome for SMEs – or is there simply a lack of interest in becoming informed? More importantly, if it is now known that there is issue with SME compliance, what are the possible regulatory responses. Should more resources be devoted to SMEs to encourage compliance? Or should DPAs come down harder on SMEs not making an adequate effort, and highlight the possible consequences of non-compliance?

[Learn more](#)



- New EP Study on the Ethics of Artificial Intelligence -

Recently, the European Parliamentary Research Service (EPRS) released a new study on the ethical issues and initiatives related to Artificial Intelligence. The study focuses, in particular, on the problems of fair benefit sharing, assignment of responsibility, exploitation of workers, energy demands in the context of environmental and climate change as well as on the more complex and abstract implications of AI – such as the impact of AI on human relationships. The study also discusses issues such as privacy, human rights and dignity, bias, and issues AI raises for democracy. The study concludes that many of the identified ethical issues are not addressed by the existing frameworks dealing with Artificial Intelligence – including those dealing with privacy and data protection. In response, the study calls for legislation and policies which will regulate the identified problems. In this regard, the study highlights that, whereas technical AI initiatives are moving forward apace, accompanying initiatives addressing identified ethical and legal problems lag behind.

[Learn more](#)



European Data Protection Board

- EDPB March Plenary Cancelled -

The EDPB Plenary Session was scheduled for the 19th and 20th of March. Owing to the Corona virus, this session will no longer take place. There is no further information on whether the agenda points for the meeting will be addressed at later meetings. There is also no further information on when the meeting will take place. Given the unforeseeable duration of the emergency measures taken to prevent the spread of the virus, it would be premature to assure that this will be the only Plenary Session which will be impacted. In this regard, there is no information as to the existence of alternative arrangements for the conduct of Plenary meetings in the case that physical meetings cannot take place for a prolonged period. One would presume the feasibility of such arrangements is being considered at the moment.

[Learn more](#)

Meet the Editors:



© FIZ Karlsruhe

Dara Hallinan, Editor: Legal academic working at FIZ Karlsruhe. His specific focus is on the interaction between law, new technologies – particularly ICT and biotech – and society. He studied law in the UK and Germany, completed a Master's in Human Rights and Democracy in Italy and Estonia and wrote his PhD at the Vrije Universiteit Brussel on the better regulation of genetic privacy in biobanks and genomic research through data protection law. He is also programme director for the annual Computers, Privacy and Data Protection conference.



© FIZ Karlsruhe

Diana Dimitrova, Sub-editor: Researcher at FIZ Karlsruhe and PhD candidate at Vrije Universiteit Brussel. Focus on privacy and data protection, especially on rights of data subjects in the Area of Freedom, Security and Justice. Previously, legal researcher at KU Leuven and trainee at EDPS. Holds LL.M. in European Law from Leiden University.

Learn more about EDPL

Recommend this newsletter. If you were forwarded this email,
subscribe here <https://www.lexxion.eu/en/newsletter/>

Lexxion Verlagsgesellschaft mbH
Güntzelstr. 63
10717 Berlin
Deutschland

+49-(0)30-814506-0

www.lexxion.eu



We sincerely apologize if you find this email an intrusion of your privacy or a source of inconvenience to you. If you would like to unsubscribe from the newsletter service, please click here: [Manage Subscriptions: \[newsletters_manage\]](#)

[Terms](#) | [Privacy](#)
