EDPL EUROPEAN DATA PROTECTION LAW REVIEW

Your biweekly news on EU data protection
For more in-depth analysis go to lexxion.eu/edpl

Data Protection Insider

Issue 22, 30 April 2020

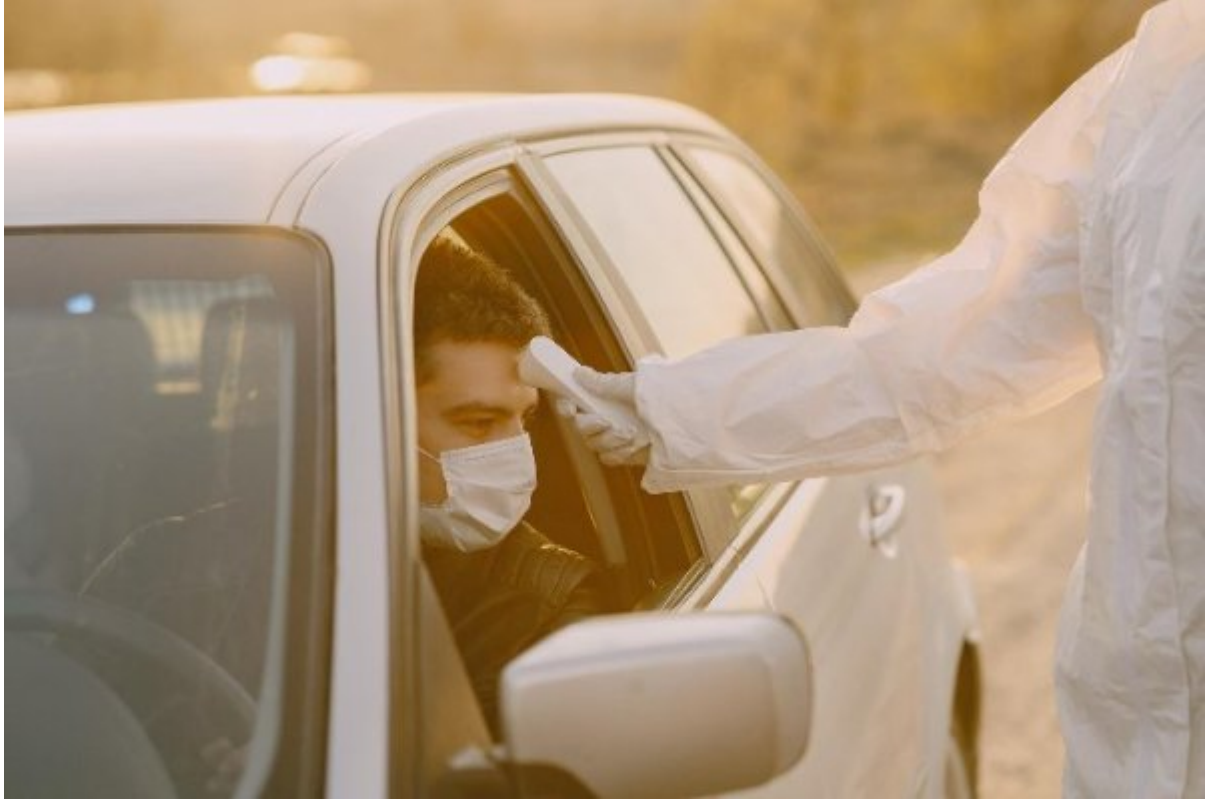
- EDPB Holds 21st-24th Plenary Sessions -

Since the 7th April, the EDPB has held four Plenary Sessions. The focus of each of these sessions has been data protection in relation to the COVID-19 outbreak. Across these sessions, the EDPB has adopted the following six documents:

- A response to a letter from the United States Mission to the European Union concerning transfers of health data for research purposes, enabling international cooperation for the development of a vaccine.
- A response to a request from MEPs Lucia Ďuriš Nicholsonová and Eugen Jurzyca concerning the applicability of data protection rules in relation to the COVID-19 outbreak.
- A response to two letters from Sophie In 't Veld MEP, concerning the latest technologies that are being developed in order to fight the spread of COVID-19.
- Guidelines on the processing of health data for research purposes in the context of the COVID-19 outbreak.
- Guidelines on geolocation and other tracing tools in the context of the COVID-19 outbreak.
- A letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic.

Documents which are not yet available on the EDBP's website should be made available shortly, following internal checks.

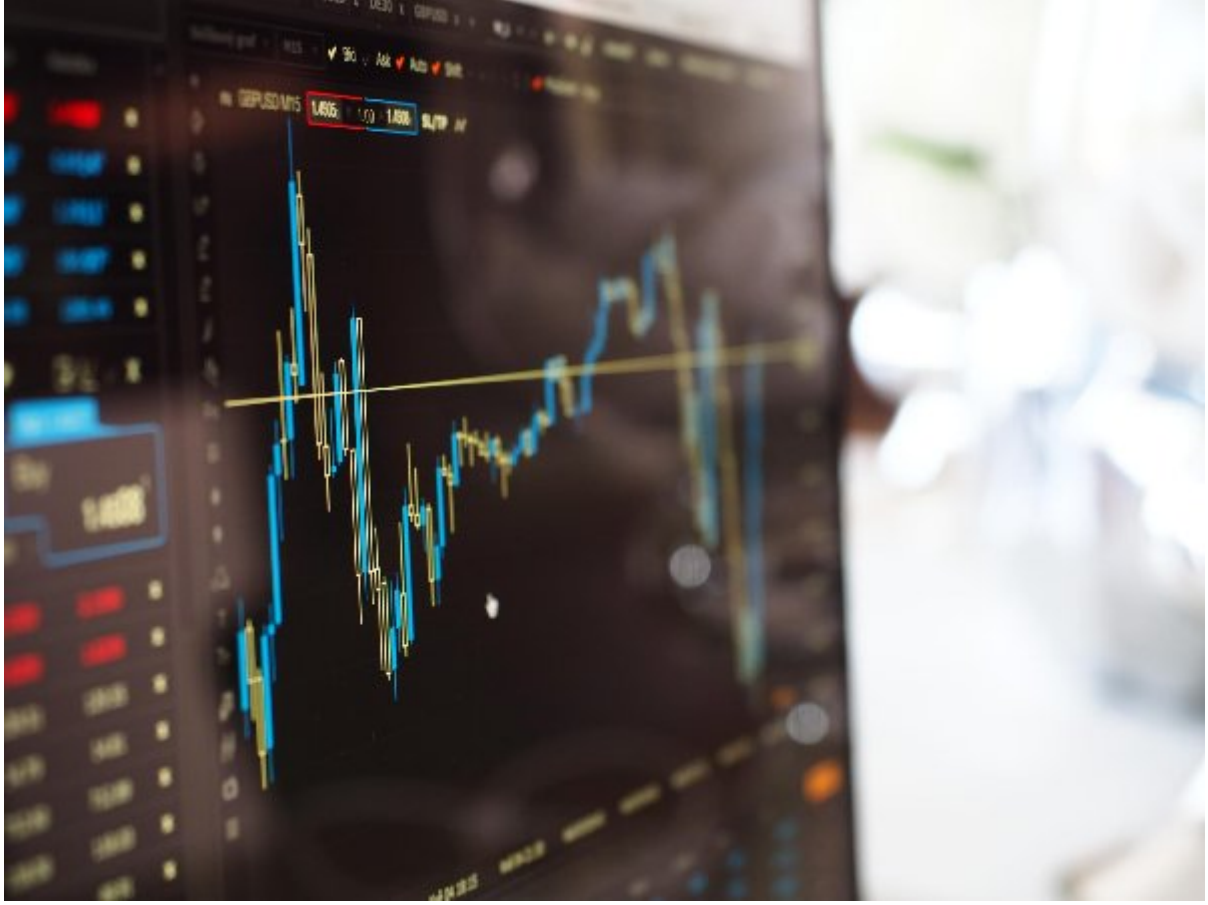
Learn more



- EDPB Guidelines on Health Data, Scientific Research and COVID-19 -

On 21st April 2020, the EDPB published a set of Guidelines on the processing of health data for scientific research in relation to the COVID-19 outbreak. The Guidelines are relatively short – at only 13 pages – and aim to provide an overview of the applicability of data protection rules to scientific research activities concerning COVID-19. The bulk of the Guidelines will thus hold few surprises for data protection experts and do not delve into many questions of law in need of clarification – for example, how secondary scientific processing should be legitimated under Article 5(1)(b) or what the concept of 'specific' national law under Article 9(2)(j) implies. Despite their general nature, the Guidelines are nevertheless worth reading. First, the Guidelines contain some novel clarifications as to the interplay between data protection and scientific research. For example, the Guidelines offer useful guidance and clarification of transparency obligations under Article 14 GDPR and as to exceptions to these obligations. Second, the Guidelines also contain certain comments likely to raise eyebrows. For example, the Guidelines assert that: 'It has to be noted that there is no ranking between the legal bases stipulated in the GDPR.' Whilst this assertion is true when one considers only the text of the GDPR, in relation to any given scientific context, other relevant legal and ethical principles will play a role in defining the appropriate legal basis.

Learn more



- EDPB Adopts Guidance on Corona Apps -

In its Plenary Meetings in April 2020, one of the topics the EDPB focused on was the deployment of apps designed to assist in the fight against the virus – including apps which aim to model the spread of the virus and contact tracing apps to inform individuals whether they have been in contact with someone infected with the virus. The outcome of discussions was a set of recommendations and guidance on app development and deployment. The key recommendations can be summarized as follows: app usage should be voluntary – this should be distinguished from the suggestion that consent is the basis for data processing; data minimisation should be ensured – for example via the anonymisation or pseudonymisation of data: the proximity of users, instead of their location, should be traced; the controller should be clearly defined; apps' functions should correspond strictly to the originally defined purpose; apps must have a legal basis for operation under data protection law – under the GDPR and, if relevant, under ePrivacy; apps should have proportionate data storage limits in place; apps should ensure the accuracy of data processing – for example, by auditing the algorithms, carrying out processing; and apps should always ensure proper security. The guidelines also stress the fact that such apps have technical limitations which should be considered. In this regard, careful consideration should always be paid to the question of how far apps can really assist public health systems. The issued guidelines are, exceptionally, not subject to public consultation due to the urgency of the issue discussed. It is yet to be seen whether, and to what degree, the Guidelines will be followed across Europe given apps have already been deployed which do not seem to conform to the above recommendations – for example because they have been designed from the outset to serve different purposes and/or because they do not include limited data storage periods.

Learn more

- European Commission Releases Toolbox on COVID-19 Contact Tracing Apps -

On 16th April, the European eHealth Network, with the support of the European Commission, released the document: 'Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States'. The document is based on the recognitions that: i) tracing apps offer potential to assist in effective contact tracing in EU Member States; ii) tracing apps deployed 'without appropriate safeguards… could have a significant negative effect on privacy and individual rights and freedoms'; and iii) '[a] fragmented and uncoordinated approach to contact tracing apps risks hampering the effectiveness of measures aimed at combating the COVID-19 crisis, whilst also causing adverse effects to the single market and to fundamental rights and freedoms'. The toolbox thus aims to provide a common orientation for Member States in the development and deployment of tracing apps, such that these apps: 'exploit the latest privacy-enhancing technological solutions that enable at-risk individuals to be contacted and, if necessarily, to be tested as quickly as possible, regardless of where she is and the app she is using.' In this regard, the Toolbox outlines a set of basic requirements for tracing apps. These requirements include, in line with those outlined by the EDPB: the requirement that apps be voluntary; the requirement that apps be approved by the relevant national health authority; the requirement that apps be privacy preserving; and the requirement that apps be dismantled as soon as they are not needed. Given the rapidly changing nature of the public health situation, as well as the rapidly changing nature of the development and deployment of tracing apps, the toolbox will be updated as necessary.

Learn more

- CNIL Launches Public Consultation on Children's Privacy -

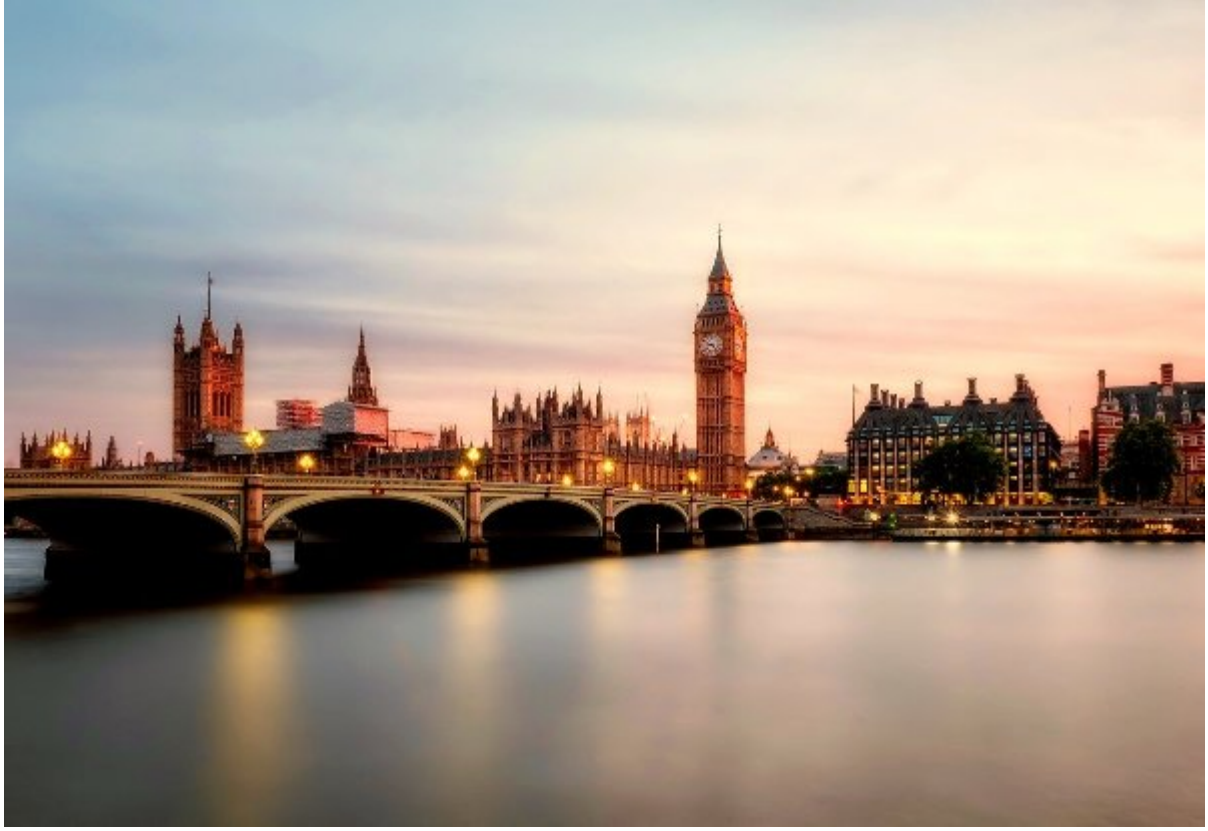
The CNIL has launched a public consultation on three topics related to children's privacy:

- The legal capacity of children to take part in online activities.

- The implementation of means to verify the age of the children and the collection of their consent.
- The exercise of children's data subject rights.

The consultation is open until 1st June 2020. Feedback will help the CNIL elaborate recommendations concerning the above topics. The consultation signals the importance of data protection matters in relation to children and minors. The questions subject to consultation remain largely unaddressed in data protection discussions – despite their importance for guaranteeing the effective protection for children. In this regard, the consultation is welcome and will hopefully trigger a productive debate leading to concrete recommendations.

Learn more



- UK Plans to Expand 'Snooper's Charter' -

The UK government is planning to give five additional public authorities – in addition to law enforcement authorities – access to the electronic data of phone and internet users under UK Data Retention legislation: the Civil Nuclear Constabulary; the Environment Agency; the Insolvency Service; the UK National Authority for Counter Eavesdropping (UKNACE); and the Pensions Regulator. The proposal still needs to be debated and voted on by the Parliament. The motivation for the proposed amendment is that these five authorities are "increasingly unable to rely on local police forces to investigate crimes on their behalf." From the Memorandum to the proposed amendments, it remains unclear why the local police forces cannot perform the investigations. On one hand, the justification could be the increase in the crimes these agencies have to deal with – for example, the Memorandum talks of 40,000 suspected environmental offences annually. On the other hand, the justification could be cuts to police forces and their reduced resources – i.e. the planned increased access to communication data might function as a compensation for the lack of police capacity. Significantly, the Memorandum does not seem to consider the data protection implications of the increased access to individuals' data implied by the proposals. In this regard, the reader may recall that there are ongoing court cases which challenge, amongst others, the legality and proportionality of access to communications data for law enforcement purposes in Europe – as previously discussed in Data Protection Insider. The outcome of such challenges will need to be considered when assessing legality of the proposed enhanced access.

Learn more

Meet the Editors:

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

© FIZ Karlsruhe

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

Lexxion Verlagsgesellschaft mbH
Güntzelstr. 63
10717 Berlin
Deutschland

+49-(0)30-814506-0

www.lexxion.eu
