PRIVACY TICKER

1. Legislative Changes

+++ BREXIT AND DATA PROTECTION: ADEQUACY DECISION IN SIGHT +++

The EU Commission has initiated the procedure for adopting an adequacy decision to allow the transfer of personal data from the EU to the UK even after Brexit. Since Brexit has been completed, the United Kingdom is a third country within the meaning of the GDPR. However, due to the Trade and Cooperation Agreement of 31 December 2020 agreed with the EU, the UK will not be considered a third country during a transitional period of a maximum of 6 months so that no additional security measures for data exchange need to be undertaken at present. To ensure that this remains possible as unchanged from 1 July 2021, the EU Commission has now determined that an adequate level of data protection exists in the UK within the meaning of the GDPR and has presented a draft of a corresponding adequacy decision.

On the draft adequacy decision

+++ NEW DRAFT OF THE E-PRIVACY REGULATION +++

The Council of the European Union has agreed on a new draft for the European Regulation on Privacy and Confidentiality of Electronic Communications (so-called "ePrivacy Regulation"). The regulation is designed to newly regulate the processing of data stored on the user's device (e.g. mobile phone or tablet) as well as communication and metadata when using online services. Among other things, the draft provides that access to a website can be made dependent on consent to the use of cookies under certain circumstances (so-called "Cookie Wall"). It is also intended that connection data can be recorded without any reason (so-called "Data Retention"). The Council's draft will be submitted to the EU Parliament in the next step.

On the EU Council's press release

+++ GERMAN FEDERAL CABINET ADOPTS TELECOMMUNICATIONS TELEMEDIA DATA PROTECTION ACT +++

The German federal government has passed a draft Telecommunications Telemedia Data Protection Act (*TTDSG*), which is intended to anticipate the trilogue negotiations on the ePrivacy Regulation (see above). The TTDSG brings together data protection provisions from the German Telemedia Act (*TMG*) and the German Telecommunications Act (*TKG*) and protects the privacy of users when using telemedia services. Information stored on a device (e.g. with the help of cookies) may only be read out with the consent of the user, unless this is necessary for the provision of the service. In addition, the TTDSG contains regulations on the processing of traffic and location data and on the secrecy of telecommunication, in particular on the so-called "digital estate".

On the legislative draft of the federal government

+++ GERMAN FEDERAL COUNCIL STOPS REFORM REGARDING ACCESS TO SUBSCRIBER DATA +++

The German federal council has refused to give its consent to the new regulation of the access to subscriber data. The legislative draft was intended to make adjustments to the "Law to Fight Right-Wing Extremism and Hate Crime" which had become necessary after a judgment by the Federal Constitutional Court (*Bundesverfassungsgericht*) (see BB Privacy Ticker of July 2020). The legislative draft was intended, among other things, to oblige telemedia providers to hand over user passwords upon request by authorities.

On the federal council's press release

2. Case Law

+++ GERMAN FEDERAL CONSTITUTIONAL COURT: MATERIALITY THRESHOLD FOR GDPR DAMAGES MUST GO TO THE EUROPEAN COURT OF JUSTICE +++

The German Federal Constitutional Court (*BVerfG*) has ruled that the unresolved legal question of whether reaching a materiality threshold is a prerequisite for compensable non-material damage under Art. 82 GDPR must be referred to the European Court of Justice (*ECJ*) for a preliminary ruling. This question has been highly controversial since the introduction of the GDPR. Various courts had recently rejected claims for damages under the GDPR by data subjects if data protection infringements had only a minor impact on the right of personality (so-called "non-material damage" (*Bagatellschäden*)). However, as the BVerfG has now

BEITEN BURKHARDT

determined, this materiality threshold does not ensue from the text of the law. The case in question concerns a judgment by the Goslar Local Court which had rejected a claim for damages due to the unlawful sending of a single advertising email.

To the decision of the BVerfG (of 14 January 2021, File ref. 1 BvR 2853/19)

+++ REGIONAL COURT OF KARLSRUHE: LOSS OF NAME, DATE OF BIRTH, GENDER, E-MAIL ADDRESS AND TELEPHONE NUMBER IS NON-MATERIAL DAMAGE +++

The Karlsruhe Regional Court has ruled – presumably before the publication of the above-mentioned decision of the BVerfG – that a GDPR damage claim does not exist in the case of mere non-material damage. The Court considered the disclosure of the plaintiff's name, date of birth, gender, e-mail address and telephone number due to a data leak to be mere non-material damage which did not cause any noticeable disadvantage for the plaintiff. The Court found the possibility of identity theft to be "abstract" and "not a particularly probable risk". The loss of transaction data also did not result in compensable non-material damage as it did not contain any compromising information.

To the judgment of Karlsruhe Regional Court (of 9 February 2021, File ref. 4 O 67/20)

+++ REGIONAL COURT OF FRANKFURT A.M.: PLAINTIFF HAS THE BURDEN OF PROOF FOR AN INFRINGEMENT OF DATA PROTECTION IN GDPR DAMAGES +++

The Regional Court of Frankfurt am Main has ruled that the plaintiff bears the burden of presentation and proof that a data leak at the responsible entity is due to a violation of GDPR obligations. In the case at hand, a data leak had occurred at the defendant. As a result, the plaintiff had received spam calls and text messages and subsequently sought damages from the defendant under Art. 82 GDPR. The court dismissed the claim because the plaintiff had ultimately only assumed, but not conclusively shown, that the data leak was actually due to a breach of duty by the defendant. It was conceivable that the data leak was due to an illegal hacker attack which the defendant and its vicarious agents did not have to expect in this form. The plaintiff could also not invoke the reversal of the burden of proof under Art. 82 (3) GDPR as this only relates to the question of fault, but not to the breach of duty.

To the judgment of Regional Court (of Frankfurt of 18 January 2021, File ref. 2-30 O 147/20)

+++ ADMINISTRATIVE COURT OF MAINZ: USE OF TRANSPORT ENCRYPTION FOR E-MAILS IS ALSO SUFFICIENT FOR PERSONS SUBJECT TO PROFESSIONAL CONFIDENTIALITY +++

The Administrative Court of Mainz has found that the use of mandatory transport encryption (SSL/TLS) for sending an e-mail containing personal data generally establishes an adequate level of protection within the meaning of Art. 32 GDPR. This also applies to persons subject to professional confidentiality, in this case a lawyer. However, if there were particular indications of an increased need for protection in an individual case, additional protective measures (such as end-to-end encryption) would have to be taken. This applies in particular to the transmission of special categories of personal data (Art. 9 GDPR) or data on criminal convictions and offences (Art. 10 GDPR).

To the judgment of the Administrative Court of Mainz (of 17 December 2020, file ref. 1 K 778/19.MZ)

+++ HIGHER ADMINISTRATIVE COURT OF LÜNEBURG: PUBLICATION OF PHOTOGRAPHS ON A PARTY'S FACEBOOK FANPAGE UNLAWFUL +++

The Higher Administrative Court of Lüneburg has ruled that the publication of a photo with identifiable persons on a party's Facebook fan page was not permissible without the participants' consent. It was true that the party had a legitimate interest in documenting that a larger number of people were politically interested in its topics. However, the presentation of identifiable persons had not been necessary. It would have been sufficient to publish an anonymised photo (e.g. with pixelated faces). According to the court, the publication of photos in social networks is associated with considerable risks due to the broad coverage.

To the decision of Higher Administrative Court of Lüneburg (of 19 January 2021, File ref. 11La 16/20)

3. Regulatory Investigations and Enforcement Actions

+++ "TASK FORCE" OF THE DATA PROTECTION AUTHORITIES PLANS TO EXAMINE THE USE OF US-AMERICAN CLOUD SERVICES BY GERMAN COMPANIES +++

According to press reports, various data protection authorities of the German states are participating in a newly formed "task force" that is to examine the transfer of personal user data to third countries by German companies. Such a transfer takes place in particular when using cloud services from US providers. The task force is to be led by the data protection authorities of Hamburg and Berlin. The transfer of personal data to the USA has been associated with considerable legal uncertainties since the so-

called EU-US Privacy Shield has ceased to apply (European Court of Justice, judgment of 16 December 2020, File ref. C-311/18 – "Schrems-II", see BB Privacy Ticker of July 2020). In response to a request from the news portal Golem.de, the Hamburg Commissioner for Data Protection and Freedom of Information, Johannes Caspar, stated that the task force is pursuing the goal of "enforcing" the requirements of the Schrems II judgment. Random inspections are to be carried out nationwide on companies suspected of using service providers from third countries.

To the report on Golem.de

To the article published in Handelsblatt (Paywall)

+++ NORWEGIAN DATA PROTECTION AUTHORITY ANNOUNCES MILLION-DOLLAR FINE AGAINST OPERATORS OF THE "GRINDR" APP +++

The Norwegian Data Protection Authority (Datatilsynet) has announced that it will issue a fine of almost EUR 10 million against the operator of the dating app "Grindr". The authority criticises Grindr for passing on data to advertising networks without having obtained effective consent from users. This is said to include sensitive data on the sexual orientation of users. In the preliminary information notice, the authority detailed why the consent obtained by Grindr did not comply with the provisions of the GDPR.

To the preliminary information on the fine (English)

+++ FINES OF EUR 250,000 AND 260,000 FOR UNAUTHORISED TELEPHONE ADVERTISING +++

The Federal Network Agency (BNetzA) has set two high fines for unlawful advertising calls in hundreds of cases. A fine of EUR 250,000 was imposed on the energy supplier mivolta GmbH because consent for advertising calls had not been properly obtained. Among other things, it was criticised that the consent declarations were not transparent and were sometimes obtained in connection with an online lottery. In another case, the BNetzA imposed a fine of EUR 260,000 on the call centre KiKxxl GmbH. Here, too, "serious deficiencies in the verification of advertising consents" had been identified.

To the press release of the BNetzA (of 11 February 2021 regarding mivolta GmbH)

To the press release of the BNetzA (of 17 February 2021 regarding KiKxxl GmbH)

+++ ADMINISTRATIVE FINE PROCEEDINGS OPENED AGAINST VFB STUTTGART +++

The State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg (*LfDI*) has opened administrative fine proceedings against VfB Stuttgart 1893 e.V. and VfB Stuttgart 1893 AG. The LfDI sees sufficient factual indications of data protection infringements in connection with a members' meeting in 2017 and individual data transfers to an external service provider in 2018. In addition, questions regarding the implementation of the current legal situation under the GDPR have also been raised. This was preceded by a review procedure lasting several months to clarify and establish the facts of the case.

To the LfDI's press release

4. Opinions

+++ EDPB PUBLISHES EXAMPLES OF SECURITY INCIDENTS SUBJECT TO REPORTING +++

The European Data Protection Board (*EDPB*) has published guidelines with 18 case studies from practice on how to deal with infringements of data security. In each case, the EDPB outlines what preventive measures would have protected against the security incident in question, what factors need to be taken into account in the risk assessment after the security incident has occurred, what measures the controller must take to reduce the risks to data subjects, and whether there is a legal notification obligation.

To the EDPB guidelines (english)

+++ BERLIN COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION: UPDATED INFORMATIVE NOTES ON PROVIDERS OF VIDEO CONFERENCING SERVICES +++

The Berlin Commissioner for Data Protection and Freedom of Information (*BlnBDI*) has conducted a brief review of various providers of video conferencing services and has updated its informative notes on video conferencing services that comply with data protection requirements. The BlnBDI examined the legal conformity of the order processing contracts provided by providers and (superficially) the technical features of the video conferencing services. One focus was on verifying whether a service exports data to third countries. The informative notes could provide guidance for controllers in selecting a secure video conferencing system. However, they do not replace the controller's obligations to examination and review. The informative notes are updated by the BlnBDI on an ongoing basis.

To the informative notes on data protection-compliant video conferencing services

If you have any questions, please address the BEITEN BURKHARDT lawyer of your choice or contact the BEITEN BURKHARDT Privacy Team directly:

MUNICH

Dr Axel von Walter
Lawyer | CIPP/E | CIPM | Licensed Specialist for Copyright and Media Law | Licensed Specialist for Information Technology Law
Axel.Walter@bblaw.com
Tel.: +49 89 35065-1321

Gudrun Hausner
Lawyer
Gudrun.Hausner@bblaw.com
Tel.: +49 89 35065-1307

Laureen Lee
Lawyer | LL.M.
Laureen.Lee@bblaw.com
Tel.: +49 89 35065-1307

FRANKFURT AM MAIN

Dr Andreas Lober
Lawyer
Andreas.Lober@bblaw.com
Tel.: +49 69 756095-582

Lennart Kriebel
Lawyer
Lennart.Kriebel@bblaw.com
Tel.: +49 69 756095-477

Susanne Klein
Lawyer | LL.M.
Licensed Specialist for Information Technology Law
Susanne.Klein@bblaw.com
Tel.: +49 69 756095-582

DUSSELDORF

Mathias Zimmer-Goertz
Lawyer
Mathias.Zimmer-Goertz@bblaw.com
Tel.: +49 211 518989-144

Christian Frederik Döpke
Lawyer | LL.M. | LL.M.
Christian.Doepke@bblaw.com
Tel.: +49 211 518989-144

Imprint

This publication is issued by
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33 | D-80339 Munich
Registered under HR B 155350 at the Regional Court Munich/VAT Reg. No.: DE811218811

For more information see:
https://www.beiten-burkhardt.com/en/imprint

EDITOR IN CHARGE
Dr Andreas Lober | Lawyer | Partner

© BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH.
All rights reserved 2021.

PLEASE NOTE
This publication cannot replace consultation with a trained legal professional.

If you no longer wish to receive this newsletter, you can unsubscribe at any time by e-mail (please send an e-mail with the heading “Unsubscribe” to newsletter@bblaw.com) or any other declaration made to BEITEN BURKHARDT.