Data security management and data protection for video conferencing software

Nicolas John · Maximilian Wellmann

Received: 1 September 2020 / Accepted: 21 September 2020 / Published online: 8 October 2020
© The Author(s) 2020

Abstract Corona crisis and video conferencing software – two terms that now belong together. However, the demands controllers have on video conferencing software can quickly reach the limits of data protection regulations. In recent years, the progressive development of video conferencing software has already excited many users and led to significant growth. In ad hoc situations, like the Corona pandemic, issues regarding data protection are all too often neglected. This is fatal considering the fact that the implementation of video conferencing software is accompanied by a large number of data protection and security issues that must be addressed and weighed up by the controller. At first glance, technically feasible solutions can quickly turn out to be “Trojan horses” and pose a serious threat to personal data. Therefore, the selection, set-up and use of data protection-compliant video conferencing software is of great importance for controllers. This article aims to examine relevant questions regarding data protection and security management from a European legal perspective. In particular, the detailed analysis of the requirements of the General Data Protection Regulation (GDPR) as well as the practical consequences for the controller should provide practitioners an overview of the legal problems associated with the implementation and use of video conferencing software.

Keywords Corona pandemic · Personal data · Video conference · GDPR · Controller · Processor

This article is based on two articles published by the authors in the “Datenschutz und Datensicherheit” (DuD) issues 8/2020 [25] and 9/2020 [26].

N. John (✉) · M. Wellmann

Institut für Medien-, Telekommunikations- und Informationsrecht (ITM), Westfälische Wilhelms-Universität Münster, Münster, Germany

E-Mail: njohn@uni-muenster.de

M. Wellmann

E-Mail: maximilian.wellmann@uni-muenster.de

Datensicherheitsmanagement und Datenschutz für Videokonferenzsoftware

Zusammenfassung Corona-Krise und Videokonferenzsoftware – ein Begriffspaar, das inzwischen zusammengehört. Was sich Anwender von der Technik wünschen, kann allerdings schnell an die Grenzen datenschutzrechtlicher Regulierung geraten. Die fortschreitende Entwicklung von Videokonferenzsoftware hat in den letzten Jahren schon viele Nutzer begeistern können und zu einer deutlichen Verbreitung dieser Lösungen geführt. In Ad-hoc-Situationen wie der Corona-Krise stehen datenschutzrechtliche Aspekte allzu gern hinten an. Dies ist fatal, wenn man bedenkt, dass mit der Auswahl der Videokonferenzsoftware viele Fragestellungen von Datenschutz und -sicherheit einhergehen, die im Vorfeld vom Verantwortlichen beleuchtet und abgewogen werden müssen. Vieles, was sich auf den ersten Blick als technisch praktikable Lösung erweist, kann sich schnell als Danaergeschenk entpuppen und eine ernsthafte Bedrohung für personenbezogene Daten bedeuten. Die Auswahl, Einrichtung und Verwendung datenschutzkonformer Videokonferenzlösungen ist deshalb von enormer Bedeutung. Der vorliegende Beitrag untersucht daher die relevanten datenschutz- und datensicherheitsrechtlichen Fragen aus europäischer Perspektive. Insbesondere wird es darum gehen, die Voraussetzungen der Datenschutz-Grundverordnung (DS-GVO) und ihre Auswirkungen auf die Praxis gründlich zu beleuchten, um Praktikern eine Übersicht über die relevantesten rechtlichen Fragestellungen zu geben, die mit der Implementierung und Verwendung von Videokonferenzlösungen einhergehen.

Schlüsselwörter Corona-Pandemie · Personenbezogene Daten · Videokonferenz · DSGVO · Verantwortlicher · Auftragsverarbeiter

1 GDPR requirements on selecting video conferencing software

General Data Protection Regulation (GDPR) compatibility of video conferencing software is essential when it comes to the protection of personal data. However, there is no reason to consider video conferencing software a priori as not compliant with the GDPR. Already at the selection stage, the controller should use the adjustment options provided by the software to ensure that the video conferencing software complies with data protection law. In this context, the complex dichotomy between the legal framework of the GDPR and the technical possibilities of video conferencing solutions needs to be resolved.

1.1 Data protection by design

According to the wording of Art. 25(1) GDPR¹ (“at the time the means are determined”), data protection law already has its say when selecting an appropriate video conferencing solution. The technical relevance implies that technology is not only

¹ All following articles without legal designation are those of the GDPR.

an element of data protection law, but also a tool to enforce it [33, Art. 25 para. 10; 3]. Although the controller usually does not develop the software in practice, this does not exculpate him from considering data protection issues as early on as at the selection stage. Art. 25(1) explicitly addresses the controller with the requirement of data protection by design. According to Art. 25(1) the fulfilment of these obligations entails two evaluations. These evaluations stipulate the controller's obligation to provide various technical and organisational measures appropriate to implement the general principles laid down in Art. 5 [2, Art. 25 para. 12].

1.1.1 Technical architecture

The first consideration is whether there is a realisable alternative to a cloud-based video conferencing software in the form of an on-premises or hybrid video conferencing solution [5, pp. 32]. From a technical point of view, on-premises solutions are centralised solutions where the content data is hosted on the organisation's own servers [5, p. 32]. The disadvantage to this solution is that, depending on the size of the organisation, a potentially large server infrastructure needs to be maintained.

In contrast to this, cloud-based video conferencing software provides a convenient way to save server capacities by processing the data by external servers [5, p. 34; 36, Art. 28 para. 2]. Although the controller has the largest influence using an on-premises solution, structural conditions may make the choice to go for software as a service (SaaS).

1.1.2 Extent of data processing

The second evaluation focuses on the question regarding the extent of the data processing. A distinction can be made between pure video conferencing solutions, which only provide real-time audio and video transmission and more advanced technologies (e.g. unified communications and collaboration [UCC]), whose functional repertoire also includes text messaging or screen sharing.² When processing personal data it must be carefully examined whether the implementation of a UCC solution with additional functionalities is compliant with the principle of data minimisation (Art. 5[1][c]). This question must be answered by the controller on a case-by-case basis and needs to be weighed against legitimate (business) purposes (Art. 5[1][b]). Nevertheless, a global decision in favour of the most data-saving solution is not appropriate with regard to the principles of data protection law [2, Art. 25 para. 18]. However, in the case of doubt, priority should be given to a more data-saving solution.

1.2 Processors

Once the controller has decided to implement an external video conferencing software, the next step is to look for instruments that enable the controller to ensure an appropriate level of data protection in compliance with the GDPR. In practice, this

² In depth [5, p. 13].

becomes particularly relevant when a transfer of personal data outside the scope of the GDPR is considered. To ensure a GDPR-compliant level in such cases, the conclusion of a processing contract is highly recommended, as it allows the controller to define a contractual (minimum) standard of data protection.³

1.2.1 Requirements

Art. 28(3) defines the requirements of such processing. At this point, it must be stressed that the software provider is legally not obliged to conclude a processing contract. Nevertheless, the requirements of Art. 25 also have an indirect impact on the processor, as Art. 28(1) obliges the controller to select the processor following the question as to whether he may guarantee processing activities compliant with the GDPR [39]. The fundamental aspect of such a contract is the consequence that the personal data remains under control of the controller and it is up to him to decide on the “how” and “why” of the processing activities, by giving instructions (Art. 28[3][a]) [40; 36, Art. 28 para. 20]. Accordingly, the activity of the processor appears as “a processing auxiliary function” for the controller [9]. Thus, the conclusion of a processing contract does not change the full liability of the controller. Therefore, it is important for both the controller and the processor to clearly define the minimum requirements of Art. 28(3) in the respective contract.

If there is a possibility of personal data being transferred to a non-European Union (EU) country, granting a permission by the controller is a mandatory part of the processing contract (Art. 28[3][a]). Art. 28(3)(c) also obliges the processor to implement all necessary technical and organisational measures in accordance with Art. 32(1). This is essential for the use of video conferencing software, as the controller himself will regularly have little influence on the technical and organisational measures taken by the processor. It is therefore even more important for the controller to secure his own high level of data protection in a contractual manner. However, in many cases video conferencing software providers will only provide unified technical and organisational measures, as the distribution of video conferencing software is a standardised mass business [23]. In fact, this practice is lawful as long as the requirements of Art. 32(1) are adequately met on the processor side, which the controller must monitor on an ongoing basis [33, Art. 28 para. 21]. Another way is the recourse to standard data protection clauses (SDPC) provided by the European Commission. In accordance with Art. 28(7), (8) these clauses may facilitate the maintenance of an appropriate data protection level, when personal data is transferred in non-EU countries [13].

1.2.2 Sub-processing

The involvement of further external sub-processors is also of great relevance. It is common to assign such sub-processors, for instance to conduct customer surveys and customer support activities [4, Art. 25 para. 10; 39]. According to Art. 28(4), the obligation for the controller arises to ensure that the sub-processor is subject

³ Concerning the dispute as to the justification of processing see [39].

to “the same data protection obligations” as those applicable between him and the processor.⁴

1.3 Transfer of personal data to a non-EU country

Most of the video conferencing software available is developed in non-EU countries, mainly the United States (US). However, Art. 3(1) states that the legal framework of the GDPR applies regardless of whether the data processing takes place in the EU [43, Art. 3 para. 1]. European data protection law is to an extent determined by the principle that its data protection level must not be “undermined” according to Art. 44(2). In addition to a legal basis for processing, a prerequisite for the transfer of data to a non-EU country is an examination of the requirements of Art. 44 in conjunction with Art. 45–47 or Art. 49.⁵ The term “transfer” thereby means any processing activity in which personal data is transferred outside the scope of the GDPR and where the place of end-use is located outside the territory of the EU [35, Art. 44 para. 3; 38, Art. 44 para. 10–12].

In the past, if personal data was transferred to the US, it was subject to the EU–US Privacy Shield, an adequacy decision under Art. 45(3). Just recently the European Court of Justice (ECJ) ruled that the Privacy Shield is no longer capable of justifying the transfer of personal data in the US [7, para. 178 et seqq.]. The ruling focuses especially on the possibility of US authorities to gain access to user data, with the consequence that the data protection level of the GDPR cannot be safeguarded [7]. In practice this means the transfer of personal data can no longer be based on the EU–US Privacy Shield. Nevertheless, the court states that transferring data is still possible using SDPC in accordance with Art. 46(2)(c). However, the recourse to SDPC is only lawful as long as the level of protection can be maintained in the US [7]. Therefore, the controller needs to take own protective measures such as encryption (which the US authorities cannot break), anonymisation or pseudonymisation of the data before the personal data processed during a video conference is transferred to the US [12, no. 5; 30, I. no. 3; 30, III. no. 1].

Alternatively, transferring data into the US might be legal under Art. 49. However, the applicability of the provision must be examined critically with regard to the derogatory nature of the provision (“derogations”) and the requirement that it can only be used for occasional transfers [20; 12, no. 8; 30, III. no. 1].

In any case, it is highly recommended to use video conferencing software processing the relevant personal data on European servers.

⁴ In depth [25, p. 509].

⁵ Concerning the dispute about the privilege of transfer in the context of processing [4, Art. 28 para. 4 et. seqq.] with further references.

2 GDPR requirements on setting-up video conferencing software (privacy by default)

Before using the video conferencing software, the next task the controller needs to address is the set-up. If the controller has decided to pick a video conferencing software with many functionalities, a further step is to examine these functions critically with regard to their necessity. Besides data protection by design, Art. 25(2) obliges the controller to data protection by default. This duty shall serve the principle of data minimisation stated in Art. 5(1)(c). The provision aims to limit the processing of personal data to a minimum [41, para. 533; 4, Art. 25 para. 17]. Respecting this principle, the controller is obliged to set up the most data-protection-friendly default settings [19]. It is not sufficient to give users the opportunity to change the data protection settings themselves, as it is evidence-based that the majority of users do not change the standard settings [1, p. 8; 33, Art. 25 para. 46]. Therefore, the principle of data minimisation is in conflict with the video conferencing software available on the market, which often provides functions that are not required to achieve the respective purpose.

Nevertheless, it would be wrong to conclude that the controller is obliged to mandatorily use the most data-efficient configuration [2, Art. 25 para. 18; 33, Art. 25 para 45b; 32, Art. 25 para. 68; 37, pp. 104]. Rather, data processing that goes beyond the minimum may be compliant with the GDPR if the respective processing has a legitimate purpose (Art. 5[1][b]) [2, Art. 25 para. 18]. The indeterminate legal term of a “legitimate purpose” is broad but can be assumed when the purpose is in line with other legal obligations [8, p. 315; 14, Art. 5 para. 6; 1, pp. 19]. The same applies to the term “necessary” in Art. 5 (1)(c), which is also an indeterminate legal term that needs to be substantiated case by case [8, p. 317; 42, Art. 6 para. 20].⁶

When using video conferencing software, the controller needs to review the appropriateness of all functions, such as the recording, observation, logging or tracking functions. This necessity test is guided by the question of whether there is not a more lenient way to achieve the legitimate purpose of the processing [21, Art. 25 para. 19; 2, Art. 25 para. 18; 32, Art. 25 para 68]. For example, if the video conferencing software provides an option between transport encryption and end-to-end encryption offering the same functionality, it is preferable to activate the latter to reduce the risk to the rights and freedoms of individuals.

The activation of a chat function also needs to be weighed up case by case. On one hand, activation might be necessary to ensure that video conference participants can communicate parallel, without interrupting the presenter. On the other hand, recording a video conference cannot per se be considered as a legitimate purpose. If the only purpose is to remember the contents of the video conference better, this purpose is not able to justify the recording, if taking (handwritten) notes is equally useful. The situation may be assessed differently, i.e. whether the exact wording of the video conference is relevant and needs to be made available to third parties.

⁶ In depth [8, p. 317].

Thus, Art. 25(2) stipulates an obligation for the controller to align the configuration of the default settings in accordance with (legitimate) purposes by deactivating functions in advance that are not required by default.

3 GDPR requirements on using video conferencing software

If the video conferencing software is pre-configured in a data protection-friendly way, the next step is to examine further relevant provisions of the GDPR governing its use.

3.1 Legal bases for processing personal data

As discussed above, during a video conference different types of personal data are processed. For example, the name and surname of the user as well as their e-mail address and other optional information are collected. In addition, the meeting metadata (topic description, participant IP address, time and date of the meeting) and the meeting content data are processed. All these different types of data may be classified as personal data if they enable a third party to identify the individual concerned.

To process personal data, a legal basis is required. Depending on the context of use, Art. 6(1)(b–f) may serve as a legal basis. A different legal basis may be considered if the processing relates to the employment of the user. Then, Art. 88(2) in conjunction with specific national provisions, for example § 26(1) of the German Federal Data Protection Act, might be applicable.

If Art. 6(1)(b–f) are not an eligible legal basis, the controller needs to consider obtaining the consent of the participants (Art. 6[1][a], Art. 7). According to Art. 4(11), consent must be given freely and prior to processing (cf. [11, p. 14 para. 43]). A key issue for valid consent is the question as to whether the data subject has a genuine and free choice and is able to refuse or withdraw consent without suffering personal disadvantages [15]. Especially in the relationship between employee and employer, the voluntary nature of consent must be examined critically due to the employer's right of direction. However, if the assessment shows that the data subject did not have a free choice and did not freely consent to processing, Art. 6(1)(a) cannot serve as a legal basis [16]. The same rules apply to consents granted in general terms, which, irrespective of the context of use, are legally invalid in accordance with the principle of purpose limitation (Art. 5 [1][b]) [8, p. 315; 22, Art. 6 para. 9]. Freedom of choice also requires that participants of the video conference are fully informed about the purpose of the data processing before giving their consent [22, Art. 6 para. 8]. Moreover, Art. 7(3) stipulates the information about the right of withdrawal.

3.2 Data security issues

While Art. 25 is taken into account when selecting and setting up the software, Art. 32 specifies the general clause of Art. 24 from the moment the video confer-

ence begins [33, Art. 32, para. 8 et seq.; 2, Art. 25 para. 16; 32, Art. 32 para. 1 & 10; 3, p. 310]. At this stage, the duty of the controller is to ensure a level of data security appropriate to the evaluated risk to the personal data of the participants [24, Art. 32 para. 1; 41, para. 541 et seq.; 6, p. 635]. In this context, the following principle applies: “The higher the risk to the rights and freedoms of natural persons, the more technical and organisational measures need to be taken” [2, Art. 32 para. 51]. By processing meeting content data, such as audio, video and text contributions, there is a potential high risk to the rights and freedoms of the participants if this data is accessed in an unauthorized way. The visual depiction of the user and the assignment of given statements to an individual indicate a significant threat to their informational self-determination. Examples in the past have shown that a lack of password protection has given third parties the opportunity to access video conference meetings with the consequence that the presented content was used in an inappropriate way against the participants [2].

Therefore, it is of great importance for the controller to adapt concrete technical and organisational measures to lower the risk of potential abuse. In cases where the software provider and the controller have entered into a processing contract, the duty to implement these measures shifts primarily to the processor (Art. 28[3][c]) [25; cf. 6, p. 634].⁷ However, with regard to the wording of Art. 32(1) (“the controller and the processor”), this does not completely disencumber the controller to organise own appropriate data security measures.

Rather, the *appropriate* measures to be taken are the result of a case-by-case weighing-up according to the criteria stated in Art. 32(1). When weighing up these equivalent criteria [33, Art. 32 para. 26], it must be borne in mind that data security measures are subject to a proportionality test [32, Art. 32 para. 1 & 10; 6, p. 635]. In some cases, this can limit the obligation to an economically reasonable extent [32, Art. 32 para. 1 & 10; 33, Art. 32 para. 60]. Controllers must also be aware that the case “Schrems II” [2] has once again significantly increased the relevance of data security measures, as the court states that, in accordance with Art. 42(2), the controller needs to take “appropriate safeguards” to legally transfer data into the US. These mentioned safeguards have a dual function as they may also be classified as technical and organisational measures under Art. 32(1)(a).

3.3 Practical guidelines

To ensure a level of data security appropriate to the risk, the following section aims to provide some practical guidelines regarding technical and organisational measures that need to be taken by the controller. However, general guidelines do not replace a case-by-case assessment of which technical and organisational measures need to be implemented with regard to the concrete risk.

Describing a first top priority, the controller should encrypt the participants’ login data stored on-premises. Furthermore, an obligatory organisational measure is the sensitisation of the employees regarding a data-saving use of the video conferencing software. How important these organisational measures can become is illustrated

⁷ In depth [25].

by the practical example of active screen sharing. It is the task of the controller to inform the users in advance to close other programmes in order to avoid the unwanted occurrence of pop-ups and thus the (illegal) sharing of personal information.

It is also useful to apply dynamic conference numbers in order to avoid third parties from entering a recurring video conference. If the software additionally provides a monitoring dashboard, the controller should activate this function to enable the organiser to find out whether there is anyone in the meeting who was not invited. Informing the organiser about the opportunity to close access to the meeting as soon as they notice that all invited people are “present” should also be on the agenda.

Despite all technical and organisational measures taken by the controller, it can be stated that a video conference is only as secure as its information technology environment. This means that both the terminal equipment and the line to the conference itself must be secured in an appropriate way. This can be done by means of data encryption, virtual private networks (VPN) and of course protection software.

3.4 Further obligations on the controller

The legal examination of video conferencing software does not end with the assessment of appropriate technical and organisational measures, but continues with an analysis of the information and reporting obligations.

When personal data is processed, the controller is obliged to inform the data subject about the ongoing processing, thereby fulfilling his duties derived from Art. 13 and Art. 14.⁸ The obligations arise when the collection of data from the data subject begins (data collected directly from the *data* subject) [34, Art. 13 para. 11]. If personal data is received from a third party, Art. 14 applies. Here, the law states clearly that information must be provided both in a precise and easily understandable manner and in clear language at the time of processing [15; 17; 34, Art. 12 para. 33 et seqq.]. With regard to these regulations, it is useful for the controller to comprehensively inform the user about the processing procedures when he/she registers for the first time. However, if the purpose or scope of the concrete data processing change, the data subject needs to be informed in advance that he/she can effectively exercise his or her right of revocation limiting further data processing (Art. 13[3]) [18; 10, Art. 13 para. 7]. This information is particularly important if functions are added (e.g. switching on a recording function), enabled or switched on after the standard functions of the video conferencing software have been set up.

Another obligation stated by Art. 15 grants the data subject a two-stage right of access to the controller regarding the question as to whether and how their personal data is being processed [35, Art. 15 para. 19; 11, p. 22]. Furthermore, the controller is subject to the reporting and notification obligations under Art. 33, 34. These provisions stipulate that both the competent supervisory authority and the data subject must be informed in the case of a breach of personal data.

⁸ In depth [31].

4 Conclusion

The analysis of video conferencing software illustrates the high level of requirements stipulated by the GDPR. Although a large number of evaluations of both a technical and a legal nature need to be carried out on a case-by-case basis, it is not impossible for the controller to select, set-up and use a secure environment for video conferencing software compliant with data protection rules. However, to declare cloud-based video conferencing software from non-EU countries as generally incompatible with the GDPR is unrealistic (cf. [28; 27]).⁹ Nevertheless, a reminder is needed to avoid an overly cavalier selection decision blinded by the wide range of technical possibilities. Here, the provisions of the GDPR operate as guiding principles.

In the first instance, the focus of the controller concerning the evaluations should be led by the question as to whether it is possible to implement an on-premises solution instead of a cloud-based SaaS solution. If this evaluation leads to the selection of cloud-based video conferencing software, questions of data security and data protection measures must be taken into account.

Here, a top priority for the controller is to deactivate by default functions that are not required to achieve the legitimate purpose. This task arises from the principle of data protection by default [41, para. 533], which also establishes the duty of the controller to permanently monitor the activated functions with regard to the question of whether they still serve a legitimate purpose. Moreover, the duties of the controller also include safeguarding data security by means of appropriate technical and organisational measures and a consideration of the requirements in terms of information, access and reporting obligations.

Summarising the results of the analysis, it can be concluded that the GDPR confronts controllers with numerous provisions, which – when implemented correctly – ensure that video conferencing software can be selected, set up and used in a legally compliant and data-secure manner.

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Article 29 Data Protection Working Party (2017) Guidelines on data protection impact assessment (DPIA). WP 248. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Accessed 16 Sept 2020
2. Baumgartner U (2018) In: Ehmann E, Selmayr M (eds) DS-GVO, 2nd edn. Beck, Munich

⁹ In the meantime, the LfDI BW sees no reason to maintain the warning regarding Zoom, see [29].

3. Baumgartner U, Gausling T (2017) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. ZD 7(7):308–313
4. Bertermann N (2018) In: Ehmann E, Selmayr M (eds) DS-GVO, 2nd edn. Beck, Munich
5. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020) Kompendium Videokonferenzsysteme. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf?__blob=publicationFile&v=4. Accessed 16 Sept 2020
6. Burton (2020) Article 32 security of processing. In: Kuner C, Bygrave L, Docksey C (eds) The EU General Data Protection Regulation (GDPR). Oxford University Press, Oxford, pp 630–639
7. Case C-311/18, Schrems II. ECLI:EU:C:2020:559
8. De Terwange C (2020) Article 5 principles relating to processing of personal data. In: Kuner C, Bygrave L, Docksey C (eds) The EU general data protection regulation (GDPR). Oxford University Press, Oxford, pp 309–320
9. District Court (Amtsgericht) Mannheim, D. f. 11.9.2019, 5 C 1733/19 WEG. ZD 10(4):206–209
10. Dix A (2019) In: Simintis S, Hornung G, Spiecker vlg. Döhmann I (eds) Datenschutzrecht. Nomos, Baden-Baden
11. EDPB (2019on) Guidelines 3/2019 on processing of personal data through video devices. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf. Accessed 16 Sept 2020
12. EDPB (2020) FAQ on the judgement C-311/18. https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjec31118_en.pdf. Accessed 16 Sept 2020
13. European Commission (2010) Decision of the European Commission of 5.2.2010 about SCCs, K/2010/593. OJ L 39 12.2.2010
14. Feiler L, Forgó N, Weigl M (2018) The EU general data protection regulation (GDPR): a commentary. Globe law and business Ltd, woking
15. Recital 39 GDPR
16. Recital 43 GDPR
17. Recital 58 GDPR
18. Recital 61 GDPR
19. Recital 78 GDPR
20. Recital 111 GDPR
21. Hartung J (2018) In: Kühling J, Buchner B (eds) Datenschutz-Grundverordnung/BDSG, 2nd edn. Beck, Munich
22. Heberlein H (2018) In: Ehmann E, Selmayr M (eds) DS-GVO, 2nd edn. Beck, Munich
23. Heinzke P, Engel L (2020) Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen. ZD 10(4):189–194
24. Hjadjk J (2018) In: Ehmann E, Selmayr M (eds) DS-GVO, 2nd edn. Beck, Munich
25. John N, Wellmann M (2020) Datenschutzrechtliche Fragestellungen zur Auswahl von Videokonferenztools. DuD 44(8):506–510
26. John N, Wellmann M (2020) Datenschutzrechtliche Fragestellungen zur Einrichtung und Verwendung von Videokonferenztools. DuD 44(9):606–610
27. Landesdatenschutzbeauftragte Berlin (2020) Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen. Note from 2.4.2020. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf. Accessed 16 Sept 2020
28. LfDI BW (2020) Communication from 29.4.2020. <https://www.baden-wuerttemberg.datenschutz.de/lfdi-gute-entscheidung-fuer-threema-schulen-brauchen-mehr-orientierung/>. Accessed 16 Sept 2020
29. LfDI BW (2020) Warnung des LfDI wurde gehört – Zoom bessert nach. Communication from 24.6.2020. <https://www.baden-wuerttemberg.datenschutz.de/warnung-des-lfdi-wurde-gehoert-zoom-bessert-nach>. Accessed 16 Sept 2020
30. LfDI BW (2020) Orientierungshilfe zu Schrems II. <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf>. Accessed 16 Sept 2020
31. Lorenz B (2019) Datenschutzrechtliche Informationspflichten. VuR 34(6):213–221
32. Mantz R (2018) In: Sydow G (ed) Europäische Datenschutz-Grundverordnung, 2nd edn. Nomos, Baden-Baden
33. Martini M (2018) In: Paal B, Pauly D (eds) Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2nd edn. Beck, Munich
34. Paal B, Hennemann M (2018) In: Paal B, Pauly D (eds) Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2nd edn. Beck, Munich

35. Pauly D (2018) In: Paal B, Pauly D (eds) *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*, 2nd edn. Beck, Munich
36. Petri T (2019) In: Simintis S, Hornung G, Spiecker vlg. Döhmman I (eds) *Datenschutzrecht. Nomos*, Baden-Baden
37. Roßnagel A, Richter P, Nebel M (2013) Besserer Internetdatenschutz für Europa. *ZD* 3(3):103–107
38. Schantz P (2019) In: Simintis S, Hornung G, Spiecker vlg. Döhmman I (eds) *Datenschutzrecht. Nomos*, Baden-Baden
39. Schmidt B, Freund B (2017) Perspektiven der Auftragsverarbeitung. *ZD* 7(1):14–18
40. Schmitz B, von Dall'Armi J (2016) Auftragsdatenverarbeitung in der DS-GVO – das Ende der Privilegierung? *ZD* 6(9):427–432
41. Schrey J (2018) General conditions for data processing in companies under the GDPR. In: Rücker D, Kugler T (eds) *New European general data protection regulation*. Beck, Munich
42. Schulz S (2018) In: Gola P (ed) *Datenschutz-Grundverordnung*, 2nd edn. Beck, Munich
43. Zerdick T (2018) In: Ehmann E, Selmayr M (eds) *DS-GVO*, 2nd edn. Beck, Munich