LG Traunstein - 9 O 173/24

From GDPRhub
Jump to:navigation, search

In a case about non-material damages, a court ruled that a controller that manages a social media platform can lawfully transfer data to the USA relying on an adequacy decision and, before the approval of the latter, on SCCs.

Contents

LG Traunstein - 9 O 173/24

Court:	LG Traunstein (Germany)
Jurisdiction:	Germany
Relevant Law:	Article 6(1)(f) GDPR Article 6(1)(a) GDPR Article 13 GDPR Article 14 GDPR Article 45(3) GDPR Article 46(2)(c) GDPR Article 49(1)(b) GDPR Article 3 Regulation (EU) 2021/1232
Decided:	08.07.2024
Published:	
Parties:	
National Case Number/Name:	9 O 173/24
European Case Law Identifier:	
Appeal from:	
Appeal to:	Unknown
Original Language(s):	German
Original Source:	Bayern.Recht (in German)
Initial Contributor:	fb

English Summary

Facts

The data subject is a user of a social network platform, which also provides a messaging service. This platform is managed by a company with its headquarter in the USA.

The data subject initiated a lawsuit before the Regional Court of Traunstein (*Landesgericht Traunstein – LG Traunstein*).

Firstly, she argued that the controller is constantly monitoring her private messages and that the privacy policy is not transparent and is too complex.

Secondly, she argued that, through cookies, the controller is collecting data relating to activities that happen outside the social network without her consent.

Thirdly, she claimed that the controller forwarded all her personal data from and in connection with her account to the USA. She argued that this transfer is unlawful since the USA did not guarantee a level of protection equivalent to the GDPR.

Therefore, the data subject asked the court to order the controller to pay non-material damages.

As for the first argument, the controller pointed out that it conducts scans on the private messages only when to detect child sexual abuse material (CSAM) in compliance with the ePrivacy Directive 2002/58/EC (see Article 3 Regulation (EU) 2021/1232).

Moreover, the controller argued that it is respecting its transparency obligations and that the transfer of data to the US is legal since there is an adequacy decision and, before that, there were SCCs.

Holding

First of all, the court ruled that the data subject has not demonstrated that the controller is systematically and automatically monitors the content exchanged via the messenger service. In every case, it found that the controller has proven that it carries out only permissible CSAM scanning. According to the court, this processing is covered by the legal basis provided for by Article 6(1)(f) GDPR.

Secondly, it held that, due to the extensive data protection requirements that are imposed on the controller, the privacy policy cannot be more concise or simpler. Therefore, it found no violation of Article 13 and 14 GDPR.

Thirdly, it did not uphold the data subject's argument about cookies. It found that the controller could rely on consent under Article 6(1)(a) and 9(2)(a) GDPR to collect this data.

Fourthly, the court noted that the social media platform at hand is designed as a global platform whose aim is to allow users to have a worldwide network and allow users to have "friends" from all over the World. Therefore, according to the court, it is obvious – and also the data subject should know this – that data is also transmitted to the USA, especially since the search for users in other jurisdictions can only work if there is a cross-border exchange of data.

Moreover, the court believed that the business decision of the controller transfer data to the USA is to be accepted by the data subject since no one is forced to use the platform.

Furthermore, it held that the data transfer at hand is necessary for the performance of a contract and, therefore, lawful under Article 6(1)(b) GDPR.

Finally, as for Chapter V GDPR, the court pointed out that currently the controller can rely on the Commission Implementing Decision EU 2023/1795 which allows data transfers to the USA under Article 45(3) GDPR.

As for the preceding period, it found that the standard contractual clauses adopted by the European commission in 2010 and 2021 according to Article 46(2)(c) GDPR provide a sufficient legal basis. According to the court, the fact the US government authorities can access the data transferred by the controller does not prevent the guarantee of an essentially equal level of protection since it is also possible for EU authorities to have such an access under Article 6(1)(c) GDPR.

Moreover, the court ruled that the data transfer is however lawful since it is necessary for the performance of the contract under Article 49(1)(b) GDPR.

On these grounds, the court dismissed the data subject's requests.

Comment

This judgement seems not to be consistent with the settled case law of the CJEU. In particular, in C-311/18, *Schrems II*, the CJEU ruled that when personal data are transferred to a third country pursuant to standard data protection clauses, a level of protection essentially equivalent to that guaranteed within the European Union must be afforded. To operate this assessment, not only the content of the SCCs must be taken into account, but also the relevant aspects of the legal system of that third country, as regards any access by the public authorities of that third country to the personal data transferred (para. 105).

In the same case, the CJEU found that the legal system of the USA does not guarantee an equivalent level of protection (paras. 198-199).

Further Resources

Share blogs or news articles here!

English Machine Translation of the Decision

The decision below is a machine translation of the German original. Please refer to the German original for more details.

Key Points:
1. The extensive data protection requirements imposed by law, including those on operators of social networks, combined with the complexity of the services regularly provided by these networks, do not allow for a concise
2. A global social network based in the USA cannot be accused of unlawful data transfer to the USA. If the social network is designed as a global platform, data must necessarily be exchanged internationally to maintain the w
3. A user of a globally operated social network cannot demand that all data of the network in question be stored and processed in Europe. The business decision of the platform operator to process the relevant data outside E

Judgment:
1. The lawsuit is dismissed.
2. The plaintiff shall bear the costs of the legal dispute.
3. The judgment is provisionally enforceable for the defendant against security in the amount of 110% of the amount to be enforced.

Order:
The amount in dispute is set at €7,000.00.

Statement of Facts:

1. The plaintiff is suing the defendant for damages, an injunction, deletion, and information due to violations of the General Data Protection Regulation (GDPR), particularly in connection with the monitoring of the ... messer

2. The defendant operates the social network "...". The plaintiff maintains a user profile there, where the name, gender, and user ID are always publicly visible, and other data provided by the user is visible depending on the s

3. The "..." also includes a messenger service through which "..." users can exchange messages and files.

4. The plaintiff claims that there is no valid consent for data processing by the defendant. The plaintiff suffers from a loss of control over their data and is concerned about potential misuse of their data. The plaintiff had provi

5. Data related to activities outside the social network ("Off-... Data") is collected, stored, and evaluated by "..." on a large scale and shared within the ... group. User consent is not obtained. The defendant has forwarded all p

6. The plaintiff requests:
1. The defendant is ordered to pay the plaintiff non-material damages as compensation for data protection violations concerning the indiscriminate monitoring of chat messages sent and received by the plaintiff via the ... r
2. The defendant is further ordered to pay the plaintiff non-material damages as compensation for data protection violations concerning the transfer and transmission of the plaintiff's personal data to the USA, particularly
3. It is declared that the defendant is obliged to compensate the plaintiff for all future damages arising from a) the indiscriminate monitoring of chat messages sent and received by the plaintiff via the ... messenger service
4. The defendant is further ordered, under penalty of a fine of up to €250,000.00 for each case of infringement, alternatively to be enforced by custodial detention of the defendant's legal representative (Director) for up to
a) indiscriminately monitoring chat messages of the plaintiff sent via the "...-Messenger" service,
b) collecting, using, and evaluating the plaintiff's "Off-... Data,"
c) transferring the plaintiff's personal data to the USA, particularly to the NSA.
5. The defendant is ordered to provide the plaintiff with information:
a) about the monitored, evaluated, and stored data from the monitoring of the ... messenger, specifically to present chat logs and disclose their internal evaluation, as well as delete this data if stored indiscriminately,
b) about which "Off-... Data" was collected at the plaintiff's IP address by the defendant and for what purpose it was stored and used, as well as delete this data if stored indiscriminately,
c) about the specific manner in which the plaintiff was affected by the transfer of their personal data to the USA, particularly to the NSA, i.e., who accessed the plaintiff's data and when, and which exact personal data of t

7. The defendant requests the dismissal of the lawsuit.

8. The defendant objects to the indeterminacy of the plaintiff's claims and the lack of interest in declaratory relief and need for legal protection. The defendant denies any data protection violation. The defendant argues that

9. The defendant further argues that it treats all messages transmitted via the messenger service confidentially. The ePrivacy Directive is followed by the defendant. The defendant conducts a so-called CSAM scanning accor

10. The defendant objects to the lack of specificity in the plaintiff's claims and the lack of need for legal protection or interest in declaratory relief. The defendant raises the defense of limitation.

11. The plaintiff had previously filed a lawsuit against the defendant under file number 9 O 989/23, including a claim for non-material damages in connection with so-called "web scraping," which was largely dismissed by a (n

12. The court held an oral hearing on the matter on 17 June 2024 and informally heard the plaintiff. For further details, reference is made to the exchanged pleadings and the hearing record.

Reasons for the Decision:

13. The partially inadmissible lawsuit is entirely unfounded.

A.

14. The lawsuit is

only partially admissible.

15. I. The Regional Court Traunstein has jurisdiction under Sections 1 of the Code of Civil Procedure (ZPO), 71(1), 23 of the Courts Constitution Act (GVG), and internationally under Article 79(2) Sentence 2, Article 82(6) GDPR a

16. II. The plaintiff's claim for a declaratory judgment on the defendant's liability for future damages is not sufficiently specific under Section 253(2)(2) ZPO. The claim for a declaratory judgment on the defendant's liability for

17. III. There is also no sufficient interest in declaratory relief (Section 256(1) ZPO) concerning the declaratory judgment claim. A declaratory interest must be denied if, from the perspective of the injured party, there is no rea

18. IV. The plaintiff's request for an injunction under point 4(a) of the claims is not sufficiently specific under Section 253(2)(2) ZPO. The word "indiscriminately" limits the request for an injunction in an objectively indetermina

19. V. The plaintiff lacks the need for legal protection concerning the request for an injunction under point 4(b). The plaintiff has the option to control the handling of "Off-... Data" or "Activities outside ... technologies" throug

20. VI. The request for deletion of "indiscriminately stored" data (points 5(a) and (b) of the claims) is inadmissible due to indeterminacy for the reasons mentioned above under point IV.

21. VII. Otherwise, the lawsuit is admissible.

B.

22. The lawsuit is – insofar as it is inadmissible, in any case – also unfounded.

23. I. The plaintiff has no claims against the defendant concerning the alleged violations regarding the ... messenger service. There is already no relevant violation of the GDPR.

24. The plaintiff has not plausibly demonstrated that the defendant systematically and automatically monitors the content exchanged via the ... messenger service in the sense of "crawling" the content. This is not evident fr

25. II. The plaintiff also has no claims against the defendant concerning the alleged violations regarding "Off-... Data."

26. 1. No data protection violation is evident in this regard either. The processing of data in connection with "Activities outside ... technologies" ("Off-... Data") is covered by the user's consent, Article 6(1)(a) and Article 9(2)(a)

27. 2. As far as the defendant may have processed "Off-... Data" without the necessary consent until the Federal Cartel Office's decision of 06 February 2019 (see press release of 07 February 2019, Annex KE-4), it has not beer

28. III. The plaintiff finally has no claims against the defendant concerning the alleged violations in connection with data transfer to the USA.

29. 1. The court cannot recognize any unlawful data transfer. The platform "..." and the MGroup originate from the USA. "..." is designed as a global platform. To maintain this worldwide network, data must necessarily be exc

30. 2. Data transfer is therefore generally necessary for contract fulfillment under Article 6(1)(b) GDPR. There are no sufficient factual indications that the defendant, as the plaintiff ultimately claims, provides its entire data s

31. 3. The defendant complies with the requirements for data transfer to third countries under Chapter V of the GDPR.

32. a) Currently, data transfer is based on the Commission's Adequacy Decision of 10 July 2023. This provides a valid basis for data transfer under Article 45(3) GDPR. Therefore, a further review of the adequacy of the protecti

33. b) For the preceding period, the Standard Contractual Clauses issued by the Commission in 2010 and 2021, in conjunction with Article 46(1) and (2)(c) GDPR, provide a sufficient legal basis. Under Article 46(1) GDPR, the d

34. c) Finally, as already stated above, the data transfer is necessary for contract fulfillment and thus permissible under Article 49(1)(1)(b) GDPR.

35. d) As far as data protection authorities hold differing views, they are not binding on the court.

36. 4. There is no conclusive evidence of a violation of Article 5(1)(f) or Article 32 GDPR. It is not apparent from the plaintiff's submissions why there should be reason to believe that the defendant does not adequately protect

37. 5. The court also cannot see a violation of Article 13 GDPR. The defendant has provided the references where the user can find information about the necessity of data transfer to foreign companies, particularly ..., Inc., as

government requests. It is not apparent that the defendant failed to fulfill its information obligation.

38. 6. As far as US government agencies, including intelligence services, can request information from ..., Inc. under US law, this is a consequence of the lawful data transfer to the jurisdiction of the United States of America.

39. IV. The plaintiff also lacks a causal damage for a claim for damages under Article 82 GDPR. During their informal hearing, the plaintiff only stated that they had been informed about possible data protection violations cor
"The fear (even more clearly: English 'fear' and French 'crainte'), in which the CJEU sees non-material damage, can only be something that the injured party (a) personally experiences and (b) mentally burdens them, thus psy

40. This is the case here: the "great concern" initially indicated only after being prompted by their legal representative during the informal hearing (after initially stating that they "also find it bad") does not constitute non-ma

41. V. The plaintiff has no claims for information against the defendant under Article 15 GDPR.

42. 1. As far as information is requested regarding the data "from the monitoring of the FMessenger," to "present chat logs and disclose their internal evaluation," the chat logs can be downloaded by the plaintiff themselves.

43. 2. As far as information is requested about which "Off-... Data" was collected at the plaintiff's IP address by the defendant and for what purpose it was stored and used, the defendant rightly refers to the self-information

44. 3. Regarding any data transferred to the NSA, the defendant can refuse to provide information because, on the one hand, there is a confidentiality obligation under US law, and on the other hand, it is inherently confiden

45. VI. The deletion requests under Article 17 GDPR (points 5(b) and (c) of the claims) are futile because they are conditional on the data processing being "indiscriminate." Even if one were to interpret this term as meaning "u

46. VII. All injunction claims fail due to the absence of a violation of the GDPR, as mentioned under points I to III. Regarding the "Off-... Data," it also adds that the user can manage the relevant settings. The plaintiff acts inco

47. VIII. In the absence of a principal claim, there is also no claim for procedural interest under Section 291 BGB.

C.

48. I. The cost decision is based on Section 91(1) ZPO.

49. II. The provisional enforceability is based on Section 709 ZPO.

50. III. The determination of the amount in dispute is based on Sections 39(1), 43(1), 48(1)(1) GKG, and 3 ZPO.

51. The court values the claims as follows:
Item / Value
1. 1,500
2. 1,500
3. a) 500
3. b) 500
4. a) 500
4. b) 500
4. c) 500
5. a) 500
5. b) 500
5. c) 500