BRANDI-DATA PROTECTION LAW DAY ON THE TOPIC "DATA PROTECTION INCIDENTS"

Information on data protection I October 2022

Introduction

On September 15, 2022 Mr. Carl Christoph Möller was a guest of BRANDI in Bielefeld. In the context of his work as in-house lawyer and consultant for data protection and data security at the consumer advice center in North Rhine-Westphalia, Mr. Möller is in charge of extrajudicial and judicial proceedings of the consumer advice center in matters of data protection law. As part of this year's Data Protection Law Day on the topic "Data Protection Incidents – Stakeholders, Consequences and Safeguards", he gave an exciting insight into various data protection law topics, current proceedings and the daily work of the consumer advice center in conversation with lawyers from BRANDI, including Dr. Sebastian Meyer, Dr. Christoph Rempe, Dr. Daniel Wittig and Dr. Christoph Worms.

During the event, issues surrounding the topic "data protection incidents" were examined from various perspectives. In the first part, the participants discussed, among other things, the term "data protection incidents", the assertion and abuse of data subjects' rights, claims for damages, and procedural aspects. To start with, Mr. Möller spoke on the topic "Legal enforcement as a consumer association in data protection – update on association action options and case study of cookies". In the second part, following the keynote speech "Uniform sanctioning throughout Europe?" by Dr. Daniel Wittig, the procedure in the event of data protection incidents, the standards for assessing fines, the role of the supervisory authorities and the cooperation between companies and supervisory authorities were discussed.

We have prepared the main contents of our Data Protection Law Day for you below.

Data protection incidents – rights and obligations of the parties involved

The first part of the event was devoted primarily to the questions of what is meant by a data protection incident and what rights and obligations arise for those involved.

Concept of the data protection incident

With regard to the question of what is actually meant by a data protection incident, Dr. Meyer first explained that the GDPR does not know the term "data protection incident" per se, but rather refers to a breach of the protection of personal data. In essence, it is understood as a matter of the improper processing of personal data. In accordance with the definition of the GDPR, this primarily includes the loss, improper use and unauthorized disclosure of personal data. As a rule, a further distinction can be made in practice between one-time incidents that have led to unlawful data processing – such as the unintended posting of one e-mail to the incorrect distribution list – and systematic non-compliance with data protection regulations – such as the deliberate and repeated failure to take security measures.

Consumer Advice Center and Data Protection Incidents

In both his keynote speech and the subsequent panel discussion, Mr. Möller reported that in the course of its daily work, the consumer advice center obtains a good overview of the data protection issues which consumers (and thus potential data subjects) are currently dealing with, and the areas in which data protection incidents are currently taking place and where consumers feel that their rights have been violated. The issues brought to the consumer advice center by consumers often concerned excessive data processing in online stores or as part of customer loyalty programs, the targeting of consumers in advertising, the use of cookies and cookie banners, and changes in data protection notices. Particularly in those areas where consumers increasingly perceive violations, the consumer advice center then becomes active in an investigative manner. Mr. Möller explained that, in addition to consumer complaints, the most frequent triggers for proceedings initiated by the consumer advice center are, on the one hand, market clearing (the discovery and prosecution of cases in which companies continue to inadequately implement issues that have already been clarified by the highest courts), and on the other, the clarification of disputed fundamental issues by the highest courts. Mr. Möller singled out the handling of cookies and the design of cookie banners as a topic that has been particularly relevant for the consumer advice center in recent times.

Example: Cookie use

Cookies are small text files used in online applications and stored on users' end devices. While some cookies are used to make certain settings available and to enable the use of an online application (technically necessary cookies), other cookies are used, for example, for tracking and analyzing user behavior (technically unnecessary cookies). Following the ECJ, the German Federal Court of Justice (BGH) ruled in its decision of May 28, 2020 (Case No. I ZR 7/16) that the active consent of the user must be obtained for the setting of cookies for the purposes of advertising or market research. Cookie banners are often used by companies for this purpose. According to the current status, these must be designed in such a way that, besides the option to accept cookies, the user also has an easily accessible option to reject them.

In response to a question from the audience as to whether a cookie banner was not necessary in the exclusive use of technically necessary cookies, both Mr. Möller and Dr. Meyer unanimously pointed out that, as a matter of principle, it was necessary to check on a case-by-case basis whether there was actually no processing of data by cookies or other technologies within the scope of the online application that required consent. If this is indeed the case, a corresponding mechanism for obtaining consent, such as a cookie banner, is also unnecessary. However, it must also be taken into account that compliance with data protection information obligations must nevertheless be observed by companies, irrespective of the necessity of a cookie banner.

Dr. Meyer also explained that the collection and processing of personal data for user analysis by other technologies (so-called cookieless tracking) also requires justification, and therefore requires a legal basis and, if necessary, consent. In addition, Dr. Meyer pointed out that in practice it can often make sense for tactical reasons to use a cookie banner regardless of its necessity, so as to avoid exposure to potential, and perhaps unjustified, accusations from aggrieved parties with regard to the absence of a cookie banner, and the corresponding effort to justify its absence.

Mr. Möller also reported on the cookie banner campaign carried out by the consumer advice centers last year, in the context of which 1,000 online presences of companies were checked to determine whether the requirements specified by the BGH had been implemented correctly. In the process, 100 data protection violations were uncovered and resolved by the consumer advice centers either out of court or in court.

Right of access and its abuse

Based on the right to informational self-determination, according to which data subjects should in principle be able to decide for themselves which personal data of theirs may be processed by which body and for what purpose, data protection law provides extensive rights for persons affected by the processing of personal data (data subjects). One of the central data subject rights according to the concept of the GDPR is the right of access according to Article 15 of the GDPR.

Dr. Meyer first explained that the right of access serves in particular to be able to find out which data about one's own person is processed by the respective controller and to check the lawfulness of the data processing process. In practice, however, according to Dr. Meyer and Dr. Rempe, the right of access is often asserted in order to express one's own dissatisfaction about other conduct of the company or to prepare the assertion of other claims (in particular claims for damages). If the right of access is asserted exclusively on the basis of such extraneous considerations, this is often an indication of its abuse. In particular, Dr. Meyer believes that abusive conduct is also present in cases in which the claim for information is asserted in the hope that it will not be properly answered in order to subsequently assert further claims against the company, in particular of a commercial nature. The GDPR itself only deals with the issue of abusiveness in the enforcement of data subjects' rights in Article 12(5) of the GDPR. However, this is exclusively about the quantitative excess in the assertion of data subjects' rights. There is no answer in the GDPR to the question of the extent to which extraneous considerations can justify the improper use of a right of access. The limits as to when abusive conduct can be assumed are still to be clarified by the highest courts. Dr. Meyer explained that the case law on the question of abusiveness has so far used various indicators, such as the reasonableness of the request for information per se and the explanations given by the person concerned in the context of the request for information. Extremely detailed legal explanations, as well as the existence of a large number of schematic requests for information from the person concerned without any concrete reason, also speak in favor of an abusive approach.

Procedure in the event of (unjustified) claims for information

Dr. Meyer reported in the further course of the discussion that he often encounters companies questioning whether they actually have to hand over documents that will presumably be used against them in the context of requests for information, and wondering how best to deal with corresponding requests.

His practical recommendation was to take information claims seriously, if only to avoid providing the other side with further points of attack. Requests for information must also be answered in principle. At the same time, the interests of the person concerned can be scrutinized. If it is determined that the person concerned only wants to "make money", the controller can block the request relatively easily. If a customer is angry about other behavior on the part of the company, customer service and a focus on the customer's actual concerns can often help.

In principle, Dr. Meyer pointed out that when answering the request for information, care should be taken not to give the impression that all available information had been provided, insofar as it could not be ruled out that further data was still available in the company. His recommendation was to explain in which systems had been searched and what data had been found. At the same time, it is a good idea to point out that more data may be stored and to ask specifically which data is of particular interest to the data subject, so that further information can be provided if necessary. In this way, legitimate concerns could often be satisfied and abusive requests averted. According to Dr. Meyer, if the motives were researched and then acted upon, a large proportion of legal proceedings could be avoided.

Dr. Meyer also referred to the role of the data protection officer to be appointed by companies. On the one hand, this person is integrated into the company and acts in an advisory capacity for it, but on the other hand he is also responsible for safeguarding the interests of the persons concerned. According to the basic idea of the GDPR, the data protection officer is the first point of contact for data subjects and can be contacted in the event of any incidents.

Example: Google Fonts

Dr. Wittig cited the reactions to a decision by the Munich Regional Court as an example of a possible abuse of rights. The court ruled at the beginning of this year that it may be appropriate to award a user non-material damages if the dynamic reloading of fonts within the framework of the use of Google Fonts results in an outflow of user data to the USA (Munich Regional Court, judgment dated January 20, 2022, Case No. 3 O 17493/20). Google basically provides for two different ways in which Google Fonts can be integrated on a page. Google Fonts can either be stored directly on the server of the site operator, or a separate retrieval from the servers at Google must be made for each user. In the latter alternative, it is necessary to disclose to Google at least the IP address of the user, which can be avoided in the first variant. Against this background, the court ruled that the dynamic reloading of content at Google for the inclusion of Google Fonts is unnecessary and thus also contrary to data protection, because there is an equivalent alternative that does not require the corresponding data transmission. The decision of the regional court has led to a regular wave of "cease-and-desist letters" in the aftermath, in the context of which targeted searches for violations in the integration of Google Fonts were carried out and claims for damages were asserted against companies.

In this regard, Dr. Meyer first emphasized that the decision of the Munich Regional Court was correct in principle. Any data processing requires the existence of a legal basis. In view of the alternative (data protection-compliant) integration option, the data transfer to Google that is at issue here cannot be based on the existence of an overriding legitimate interest. In the case on which the decision was based, no abuse of rights could be identified, and it was at least debatable whether the person concerned had actually suffered a loss in relation to his privacy if he had the corresponding personal attitude.

However, he also pointed out that the decision was subsequently misconstrued, and a business model was developed that did not meet the objective of data protection law. In the meantime, people are specifically looking for pages on which the fonts are still incorrectly integrated in order to subsequently assert claims for damages against the respective companies. Insofar as an allegedly affected party exclusively asserts a claim for damages in the context of its inquiry, while a claim for injunctive relief is not mentioned at all, an abusive request can be assumed with relative certainty. Even if the damage was provoked by the person concerned through the targeted search for an infringement and the infringement was even "discovered with pleasure", in Dr. Meyer's view there is no room for a claim for damages. In these cases, the provoked damage is rather only a necessary prerequisite for the claim for damages.

Public law perspective on data protection incidents - fine proceedings

The second part of the event focused on the public law perspective on data protection incidents, with particular discussion of fine procedures and the role of supervisory authorities.

Uniform sanctioning throughout Europe

In his introductory speech, Dr. Daniel Wittig first pointed out the high fine framework of the GDPR, according to which a fine of up to 20 million euros or 4 percent of a company's global annual turnover can generally be imposed for data protection violations. Whereas the data protection supervisory authorities were initially reluctant to impose fines following the entry into force of the GDPR on May 25, 2018, there has since been an increase in the frequency and amount of sanctions.

The GDPR does not contain any explicit provisions on the calculation of fines. However, according to Article 83(1) of the GDPR, they should be „effective, proportionate and dissuasive". In order to increase transparency in the assessment of fines and to ensure a uniform approach by the various supervisory authorities, the Data Protection Conference (Datenschutzkonferenz, DSK), the body of independent German federal and state data protection supervisory authorities, published a concept for the assessment of fines in proceedings against companies in October 2019, which was applicable to situations within Germany. The DSK's concept will now be superseded by the new Guidelines on the calculation of administrative fines under the GDPR, which the European Data Protection Board (EDPB), an association of representatives of national data protection authorities and the European Data Protection Supervisor, published on May 12, 2022. The guidelines are intended to harmonize the calculation of fines across Europe, as they also apply to cross-border cases in the European Union. Similar to the concept of the DSK, the amount of a fine is determined in five steps according to the new guidelines, which Dr. Wittig explained in his presentation. We have provided details on the calculation of fines according to the EDPB guidelines in the main topic of our data protection newsletter in September 2022.

In his presentation, Dr. Wittig emphasized that the new guidelines are fraught with problems. For example, it is problematic that the turnover of a company is decisive for the amount of the fine, although the GDPR itself is only based on offence-related criteria and not on turnover, and the ECJ has already determined for antitrust law that turnover should not be accorded excessive importance in the determination of sanctions. Moreover, no mitigation was provided for a first offense and the authorities continued to have a wide margin of discretion in classifying the severity of the offense and determining the penalty catalogs.

As a conclusion, Dr. Wittig stated that although the guidelines represent an important element for the uniform application of the GDPR and allow more flexibility than the concept of the DSK, they are not a fine calculator. An evaluation and revision of the guidelines is also planned by the EDPB itself.

Role and position of data protection supervisory authorities

The panel discussion that followed the keynote presentation began with a conversation about the role and position of the data protection supervisory authorities. Dr. Worms outlined the various tasks and powers of the authorities under the GDPR. He pointed out, for example, that the authorities record data protection violations. In addition, they would have a clarification and advisory function and would work to ensure that violations are remedied at the responsible companies. They have the possibility of issuing notices and decisions to responsible bodies, i.e. administrative acts, against which responsible persons can defend themselves before the administrative courts. Ultimately, however, the supervisory authorities are also responsible for punishing violations by imposing fines. In Dr. Worms' opinion, the supervisory authorities usually act with a sense of proportion in this regard, although there are differences between the individual authorities.

Abusive assertion of data subject rights

With regard to the public law perspective on data protection incidents in the second part of the event, the participants also discussed the abusive assertion of data subjects' rights. Regarding the question of which cases data subjects' rights are abusively asserted in, Dr. Worms pointed out that there are differences in case law in this regard. While the objection of abuse of rights tends to be rejected in the case law of the labor courts, some civil courts have already affirmed cases of abuse of rights. There is still no case law in this respect from the area of administrative law.

For the law on freedom of information, a similar area, Dr. Worms pointed out that in the meantime it had already been conclusively clarified before the German Federal Administrative Court that the objection of abuse of rights could only be raised in special exceptional cases with the demonstration of completely disapprovable, evident motives. In this respect, he explained that the area of the right of access under data protection law is just as independent of motives and purposes and that, according to the previous indications of the administrative courts, these are of a similar opinion and would also deny an abuse of rights in principle.

Dr. Rempe argued that the objection of abuse of rights is derived from the prohibition of excessiveness and the principle of proportionality in European law, and that the purpose of the right of access according to the recitals of the GDPR is precisely to determine whether someone's personal rights are affected.

Dr. Meyer reiterated that the right of access is intended to enable the data subject to decide on the lawfulness of the processing of his or her personal data. In his opinion, it is therefore possible to

abuse the right of access. In practice, it is the task of the data controller to prove the abuse of rights. When gathering evidence, it is also helpful to exchange information with other data controllers in order to find out whether they are affected by the same request for information. From Dr. Meyer's point of view, however, it would be desirable for the supervisory authorities to more clearly reject requests that are evidently querulous. In principle, however, it is to be welcomed that the authorities initially take every request from a citizen seriously and decide on it irrespective of the motives.

Mr. Möller reported that many inquiries that reach the consumer advice center are based on the fact that it is unclear to consumers where a company has obtained their data from, how their data is processed, and to whom the data is passed on. He therefore expressed caution in the hasty assumption of an abuse of rights, which is usually not the case. In his view, this follows from the central role of the right of access in the GDPR, which often makes the assertion of further rights possible in the first place.

Procedure in the event of data protection incidents
Another topic of discussion was how data controllers should ideally proceed in the event of a data protection incident. Dr. Worms began by recommending that data controllers observe the deadline for reporting a data protection incident to the supervisory authority, which according to Article 33(1) of the GDPR must be done within 72 hours of becoming aware of the incident. In this context, being aware does not mean that the incident must already have been conclusively investigated; rather, it is based on the point in time from which the possibility exists that personal rights have been violated. The time limit can also expire over a weekend. In this respect, it is also important for companies to clarify their own role. In order to find out who is subject to the notification obligation, it must first be clarified whether the company is solely responsible for data processing or jointly with another company, or whether it is a processor.

Dr. Meyer pointed out that, in order to comply with the tight notification deadline, it is imperative to draw up a concept for the procedure in the event of data protection incidents in order, for example, to define internal information chains in advance. It should also be noted that not every data protection violation is subject to notification, but that the notification obligation is based on the existence of a risk or, in the case of the obligation to notify affected parties, a high risk to the rights and freedoms of natural persons. In this context, the probability of occurrence and the potential impact on the data subjects must be taken into account. In this respect, the assessment is to be made on the basis of a forecast. Dr. Worms pointed out in this regard that a forecast that was once justifiable, but which in retrospect turns out to be incorrect, does not necessarily mean that there has been a data protection breach.

Dr. Meyer added that there is a function in the reporting portals of the supervisory authorities to save and document an incident that only leads to a low risk and is therefore not subject to mandatory reporting. If the incident leads to a different risk assessment at a later date and thus to a notification obligation, the document can serve as proof that a different assessment was previously made with regard to the severity of the breach.

When reporting data protection incidents, it should also be taken into account that the authorities receive a large number of reports and that the employees there usually have little time to process them. For practical purposes, Dr. Meyer therefore recommended that all relevant information be sent directly to the supervisory authority, if possible within the deadline. The possibility of preliminary notification and subsequent submission of information should only be used if the notification deadline cannot otherwise be met.

Dr. Meyer pointed out that involving the supervisory authority in the question of whether a breach was reportable is also a possible course of action. In this case, however, the responsible body should be prepared to implement the measures proposed by the supervisory authority at the end.

Cooperation of the consumer center with the supervisory authorities
In this context, Mr. Möller reported on the cooperation of the consumer advice center with the supervisory authorities. In this respect, there is regular coordination with the data protection supervisory authority in North Rhine-Westphalia. Mr. Möller welcomed the fact that the supervisory authorities are now presenting their own positions to the public, since the statements and resolutions are also relevant for the consumer advice center. However, in his opinion, it would be desirable for these legal positions to be enforced more strongly vis-à-vis companies as well. This could be done, for example, by means of administrative acts and possible confirmation by the courts, which would make a considerable contribution to legal certainty.

Enforcement practice of the supervisory authorities
In connection with the enforcement of the positions of the supervisory authorities, the discussion was directed to the enforcement practice of the supervisory authorities. Dr. Meyer pointed out that the threat of fines had so far been seen as an incentive to implement the orders of the supervisory authorities.

In the opinion of Dr. Worms, the reason for this is a problem of enforcement law, since although general enforcement law is actually available, the notices cannot be enforced on their own. In the case of administrative enforcement, the only conceivable measure was a penalty payment, which, however, was smaller than a fine and therefore less effective, albeit with a different purpose.

Dr. Meyer saw it as a weak point that on the one hand the supervisory authorities can be called in for consultation purposes and on the other hand fine proceedings are possible, but the middle ground between these two possibilities still has to be filled. It would be desirable to clarify issues independently of sanctions.

Procedure of controllers with regard to possible sanctions
In order to defend oneself against sanctions, Dr. Worms recommended taking advantage of the opportunity to be heard before the penalty notice is issued in order to present one's own position. A controller can take legal action against a decision, although a certain amount of time must be expected before a decision is reached in the second or third instance.

With regard to the imposition of sanctions, Dr. Meyer pointed out that it is difficult for companies to calculate fines and "accept" them in their own actions due to the high level of fines. Even if the new guidelines of the EDPB have led to an improvement in the calculation of fines, there are regularly doubts about the proportionality of the fines, a fact that can be attributed to the weaknesses of the concept of fines, in particular the great importance of the turnover of a company. In this respect, it remains to be seen how the courts will rule on fines that are calculated in future on the basis of the new guidelines. At least so far, the supervisory authorities have not been successful, or at least not predominantly successful, in defending their fines in court.

Conclusion

At our Data Protection Law Day, the participants in the event took a stand on various data protection law issues relating to the topic “Data protection incidents – Stakeholders Consequences and Safeguards”. They made it clear that, on the one hand, responsible parties can take appropriate measures to minimize the risks of an incident and optimize procedures in advance in the event of an emergency, and that, on the other hand, the EDPB‘s guidelines on the assessment of fines and various statements by the supervisory authorities have in some cases already created greater legal certainty with regard to possible sanctions. For some topics, however, future clarification remains to be seen. This relates in particular to the revision or judicial review of the calculation of fines and the stronger positioning and enforcement of positions by the supervisory authorities.

Christina Prowald/Johanna Schmale

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M johanna.schmale@brandi.net