

8/2021 Supplement

HERAUSGEBER

RAin **Dr. Astrid Auer-Reinsdorff**, FA IT-Recht, Berlin/Lissabon/Vorstand Deutscher Anwaltverein – **Prof. Dr. Nikolaus Forgó**, Professor für Technologie- und Immaterialgüterrecht und Vorstand des Instituts für Innovation und Digitalisierung im Recht, Universität Wien – RAin **Prof. Dr. Sibylle Gierschmann**, LL.M. (Duke University), FA Urheber- und Medienrecht, Hamburg – RA **Prof. Dr. Christian-Henner Hentsch**, M.A., LL.M., Leiter Recht und Regulierung beim game – Verband der deutschen Games-Branche e.V., in Berlin/Professor für Urheber- und Medienrecht an der Kölner Forschungsstelle für Medienrecht der TH Köln – **Prof. Dr. Thomas Hoeren**, Direktor der Zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. Dr. Bernd Holznagel**, Direktor der Öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Dr. Christine Kahlen**, Leiterin der Unterabteilung VIB, Nationale und europäische Digitale Agenda, Bundesministerium für Wirtschaft und Energie, Berlin – **Dr. Dennis-Kenji Kipker**, Wissenschaftlicher Geschäftsführer am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen, und Mitglied des Vorstands der EAID, Berlin – **Wolfgang Kopf**, LL.M., Leiter Zentralbereich Politik und Regulierung, Deutsche Telekom AG, Bonn – **Prof. Dr. Marc Liesching**, Professor für Medienrecht und Medientheorie, HTWK Leipzig/München – **Dr. Reto Mantz**, Richter am LG, Frankfurt/M. – **Prof. Dr. Alexander Roßnagel**, Universität Kassel/Leiter der Projektgruppe verfassungsträgliche Technikgestaltung (provet) – RA **Dr. Raimund Schütz**, Loschelder Rechtsanwältin, Köln – **Prof. Dr. Louisa Specht-Riemenschneider**, Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht, Rheinische Friederich-Wilhelms-Universität Bonn – RA **Dr. Axel Spies**, Morgan, Lewis & Bockius LLP, Washington DC – **Prof. Dr. Gerald Spindler**, Universität Göttingen

BEIRAT DER KOOPERATIONSPARTNER

Alisha Andert, Vorstandsvorsitzende des Legal Tech Verband Deutschland e.V., Berlin – **Daniela Beaujean**, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Medien (VAUNET), Berlin – RAin **Susanne Dehmel**, Mitglied der Geschäftsleitung Bitkom e.V., Berlin – **Dr. Andrea Huber**, LL.M. (USA), Geschäftsführerin, ANGA Verband Deutscher Kabelnetzbetreiber e.V., Berlin

REDAKTION

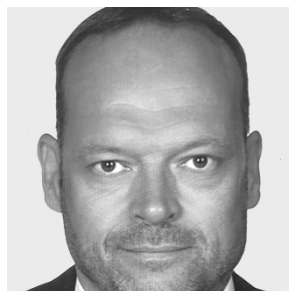
Anke Zimmer-Helfrich, Chefredakteurin – **Katharina Klauer**, Redakteurin – **Ruth Schrödl**, Redakteurin – **Eva Wanderer**, Redaktionsassistentin – Wilhelmstr. 9, 80801 München

EDITORIAL Creative law for a creative industry

reading time: 9 minutes

When creativity meets law and regulation, it opens infinite horizons for lawyers. This especially holds true for the computer games industry. For more than 20 years, lawyers all over the world have been dealing with the special legal issues of this industry. In this they encounter all kinds of legal fields, even those that do not initially appear to be of particular relevance in this context: The challenges range from questions of the permissibility of state aid to aspects of sales tax and withholding tax, foreigners' law, but also export control or the permissibility of requests for information by law enforcement agencies.

In addition, there are the „classic games law topics“, such as copyright, patent law, data protection law, youth protection law, consumer protection law, antitrust law, etc. A special focus also lies on the enforcement of the rights of market participants, primarily developers and publishers of games. Since these are located or active both in Germany and abroad, legal issues arise not only under national and EU law, but also in other legal and cultural spheres. One example might be the initially exotic question of the extent to which certain terminology and designations of objects in computer games are inadmissible in other countries for cultural, religious, or legal reasons. Such aspects have a particular influence on international youth protection law.



Tobias Haar

In addition to written „state“ law, the area of „soft law“ set by, for example, app platforms or gaming platforms is becoming increasingly relevant. Examples include the app tracking transparency function recently introduced by *Apple* or the Google Safety Section. In most cases, game providers miss a level-playing field vis-à-vis these powerful platform providers for negotiations. Often, the regulation of national law on general terms and conditions are of little help here, if the corresponding contracts are subject to US law, for example.

At the same time, „national“ legal acts, such as the GDPR, remain applicable and take precedence over this form of „private legislation“. Questions therefore arise at several levels of competing regulations. Conflicts are inevitable and solutions are sometimes difficult to be found.

It continues to be regrettable that questions and basic features of contract drafting and negotiation play an all too subordinate role in legal education in this country. All „games lawyers“ need to have appropriate experience in this area. Complex co-publishing contracts, contracts with influencers, eSports providers and eSports players are just as much a recurring topic as questions of corporate contract law, for example in founding or participating in development studios in Germany and abroad. Tax

law issues are of central importance, especially in these areas. Here, competencies are required that all too often only must be learned and adopted from scratch after successfully passing the Second State Examination in Law.

The above-mentioned legal challenges demand a special understanding of the technical and other processes of computer games as well as the economic interests of the market participants from in-house lawyers or consulting lawyers working in the games industry – and this not only for answering questions of antitrust law. Especially in the drafting of contracts, „creative law“ is often required, for example, when new forms of appropriate sharing of marketing revenues between game developers and publishers are to be developed and translated into contractual language.

Now in its fourth year, MMR is making an important contribution to both the (legal) scientific examination and the discussion of practical solutions with its annual supplement on law and games. The following emphasis topics of the games industry were previously focused on: 2018 Law of eSports, 2019 Law Enforcement, 2020 Law for the Protection of Minors. As shown, there is material for many more.

The subject of this supplement, data protection law, is of particular relevance to computer games. Nowadays, they are either mostly client or browser games with online functions or are downloaded and played as smartphone apps. The number of computer games that can be played purely offline is constantly decreasing – but they still exist. Data protection law already comes into play when a game is downloaded for the first time. This does not even have to have in-game online functions to trigger data protection issues. They then accompany the game provider beyond the user's use of the game.

There is no doubt that the GDPR has cast a spotlight on data protection law. On the one hand, nothing has changed in terms of the principle of no processing of personal data unless for a reason justified under statutory law, but on the other hand, this area of law has undergone a major shift towards increased responsibility on the part of the controllers and processors – with both advantages and disadvantages. The significantly increased catalogue of fines and sanctions does the rest to achieve the desired increase in attention.

The GDPR went into effect with a big bang a good three years ago. Countless hours of legal work have gone into compliance programs and the education and training of other departments. In the meantime, however, disillusionment has set in and statements such as „100% data protection compliance is not possible and must now be accepted“ are not uncommon. Regulation in the form of a GDPR must work with vague legal terms. Lawyers are used to dealing with the associated challenges.

But if we add to this the fact that data protection regulators in several countries often take different approaches and sometimes a greater or lesser interest in law enforcement, characterized by different funding concepts and political influence, and tend to act with or rather against the providers of computer games (and of course other areas), an international industry faces major problems. The computer games industry suffers greatly from the inconsistent application and interpretation of data protection law requirements, not only under the GDPR within the EU, but beyond. In data protection law, waiting for

clarifications from the *ECJ* is unfortunately becoming a permanent state of affairs. And once it has finally ruled, as in the Schrems II judgment, the uncertainties do not end, but sometimes only begin. The Brexit was not helpful in this context either.

MMR does justice to the importance of data protection and the legal discussion for the games industry with this supplement and the selected topics. For years, the authors have been united by an open culture of exchange and discussion in the form of working groups or lawyers' meetings at gamescom and the like. Their meetings are prepared and held with great dedication and energy – in times of pandemic, the industry in its virtual events benefits from the previously established, sometimes close friendships that have become indispensable and still manages to attract and integrate new members for their working groups.

These working groups, in particular of *game – Verband der deutschen Games-Branche e.V.* were and are indispensable for gaining as uniform an understanding as possible of legal issues. They also enable in-house lawyers to draw on a wealth of knowledge in – as described – even exotic areas of law when resources in legal departments are scarce. They also make it possible to engage in exchange with politicians as well as other industries and their associations. And all this not only on a national, but also on an international level, as successful event formats (e.g., the Games Industry Law Summit in Vilnius) impressively demonstrate. With its merger of G.A.M.E. and BIU a good three years ago, *game* has gained in importance in this area. Who would have thought how successfully these working groups would develop when a few in-house lawyers agreed to exchange experiences on the correct value-added taxation of later so-called „electronically supplied services“ more than ten years ago and jointly contacted the *Federal Ministry of Finance*?

I take great pleasure in my role as spokesperson for the *Legal Working Group at game*. I share friendships with numerous participants and a desire to discuss and broaden my horizons on the many legal topics in the industry. We can draw on a wealth of professional and life experience. Our discourse is broadly based on in-house lawyers and attorneys, institutions such as the *Entertainment Software Self-Regulation Body (USK)*, and the *game* and its members. Special praise is due to the association's office and its head of law & regulation, the co-publisher of MMR and initiator of the supplements *Christian-Henner Hentsch. As „AG Recht des game“*, we will continue to hold workshops on data protection and many other legal topics – in German and English. Most recently, for example, we have dealt with webinars around legal issues of Brexit or law enforcement. And in the coming year, we as „Games Lawyer“ will again be happy to contribute to another focus issue of MMR.

We invite all interested parties to join us in continuing and further intensifying this fruitful discourse and exchange. There is no shortage of topics for future issues of MMR, as the soon to be published „Handbuch Games und Recht“ (Games and Law Handbook) will impressively prove. So, it remains exciting in „games law“ – very exciting.

Berlin, August 2021

Tobias Haar

is spokesman for the legal working group at *game – Verband der deutschen Games-Branche e.V.* and an attorney-at-law in Karlsruhe.

Data processing in the video games industry

The gaming experience between contract performance, legitimate interests and consent

Data usage

Data is collected and processed in a video game for many different reasons: to enable game play and communication in multiplayer mode, to purchase and provide content, to improve the game experience and develop new games, or even for advertising purposes. Most of these data processing operations are carried out because the processing is necessary for the performance of a contract, for compliance with a legal obligation or for pursuing legitimate interests; only rarely consent

is required. After three years, the GDPR has been firmly implemented in the daily working practice and many „best practices“ have emerged. The harmonised regulations have proven their worth, even if the provisions on tracking and data transfers to third countries as well as different interpretations by the European supervisory authorities continue to cause problems.

reading time: 22 minutes

I. Introduction: The importance of data for the video games industry

Data is the lifeblood of the video games industry. The sector depends on data of its users to enable an interactive gameplay experience and, above all, to constantly improve and optimise this experience according to the gaming habits of its users. Data protection law has become of central importance to the industry. As there are no specific regulations for video games, the GDPR, the Federal Data Protection Act (BDSG), and incidentally also the Telemedia Act (TMG) must be applied when personal data is processed. When applying these rules, consideration should be given to the respective business models to establish which types of data are collected and processed. As most video games now have an online connection, personal data is almost always collected. Data is processed in particular for the provision of the gameplay service, for billing purposes and to improve the player experience. The use of personal data for advertising or advertising-based refinancing is, however, not as common in the video games industry as it is in other media sectors. In this respect, the games industry has different business interests, and thus also different legal challenges.

In order to map out these specificities, this article will first describe what types of data are typically collected, processed and stored in a video game (II). It will provide an overview of the central role that data plays in the value chain and explain which types of data are so essential that a game would not function without it. Subsequently, the legal grounds for lawful data processing according to Art 6 GDPR will be explained whereby we will focus on consent and consent in the context of minors, in addition to the processing necessary for performance of a contract and for the pursue of legitimate interests (III). Finally, the last chapter will feature specific aspects related to tracking, commissioned or joint data processing and data transfers to third countries (IV).

II. Data processing in the video games industry

As a business model, the essence of a video game is to provide a digital and interactive service to satisfy the player experience. To deliver this service to the player, several categories of data are required. Typically, but not exhaustively, purely functional and technical data is collected and processed, such as account data, gameplay data, communication and interaction data, and data from third parties.¹

1. Device and network data

For every video game – whether on a PC, console or mobile device – a connection between the servers of the provider and the device of the player needs to be established. This requires the collection and processing of technical information related to the configurations of the network, the device and the connected peripherals such as controllers and headsets. Examples of such device and network data include MAC and IP addresses, device serial numbers, internet service provider or mobile carrier data, etc. This type of data may also encompass information about the software or applications that are installed on the device and how they are used by the player.

Although of a technical nature, this type of data should be considered personal data as it may allow to reveal the identity of the player directly or indirectly. In the latter case, the ability of a third-party to lawfully combine the data with complementary identifiable information should always be presumed if such an activity would constitute a „means likely reasonably to be used“.² The collection and processing of this type of data often requires direct access to information and processing and storage capabilities of the device of the player by using cookies or similar technologies and is then subject to different legal requirements under ePrivacy law.

2. Account data

Joining an online gameplay service usually requires registration of an account whereby, at minimum, basic contact information and profile information is provided by the player in addition to choosing a username and password of choice. While names and e-mail addresses are always processed upon registration, age is often also collected to comply with relevant data protection and minor protection rules.³ In some cases, the free use of an online game only requires an e-mail address, username and password. However, to enable the purchasing of content, essential billing

¹ See for example the Nintendo Privacy Policy, which lists categories of data, available at: https://accounts.nintendo.com/term/privacy_policy/US?lang=en-US and in great detail the EA Privacy Policy, available at: <https://tos.ea.com/legalapp/WEBPRIVACY/DE/de/PC/#section1>.

² Cf. on dynamic IP addresses *ECJ* MMR 2016, 842 m. *Moos/Rothkegel* – Breyer.

³ In line with the principle of data minimization, it is recommended to merely inquire whether a certain age has been reached. In the case of a more continued use of a service, however, this should be determined more explicitly with the exact date of birth which is also a requirement to comply with minor protection rules.

information such as the physical address and credit card number is needed as well. Finally, telephone numbers may also be processed in addition to the name, address and e-mail for the processing of enquiries and customer support. Account data can contain sensitive information and is often linked to other personalised information about popular game titles, scores and achievements, communication and marketing preferences, etc. Usernames or gamer tags are a commonly used form of pseudonymised data and allow players to interact with each other while protecting their identity. Passwords are usually stored in a hashed form which does not allow to reconstruct the actual password.

3. Gameplay data

As players interact with video game content or with other players, data about their activity is generated. This data plays an essential role in the way companies are detecting software errors or bugs and fraudulent behaviour by the players. It is also used to improve the user experience, for example to find bottlenecks within the game, where many players fail the tasks at hand. By collectively analysing players' data, a video game company can identify if there is a large problem being experienced by the majority of the players and learn how it needs to be fixed. Developers and publishers therefore regularly provide updates and patches to games that add to and improve existing content and user experiences. Analysis of gameplay data also helps match players based on non-precise location and their skill without having to further identify them. Players have a more enjoyable experience if they are matched with other players of similar skill levels and the location is required to ensure that players are placed together on the most appropriately located servers to prevent their connections from being interrupted. Similar to device and network data, gameplay data may, often only indirectly, allow to reveal the identity of the player and should then be considered as personal data.

4. Communication and interaction data

Gameplay services generally include communication features within the game software that enable communication between players or between the player and the provider of the service. Such ancillary communication services support the gameplay activities by allowing players to plan a gameplay session ahead and communicate during gameplay. They also allow the player to report malfunctions, inappropriate content or abusive behaviour.⁴ Communication with the provider may occur outside the game software where it is necessary to respond to requests, provide product support, or enable membership features, such as the ability to receive exclusive content, redeem prizes for competitions, or receive newsletters. The content of a communication as well as the related metadata processed for the purpose of its conveyance may reveal very sensitive and personal information and is therefore subject to strict confidentiality requirements. Communication services in video games, such as a chat function in an online game, are not regularly considered as an interpersonal telecommunications service according to § 3 No. 23 Telecommunication Act (TKG) because they are ancillary to another service.⁵ However, it should be pointed out that the data protection regulations of the Telemedia Act and, in the foreseeable future, the new rules of the currently still negotiated ePrivacy Regulation apply here. According to the planned revision of the ePrivacy Directive, it will probably be no longer possible in the future to actively or reactively monitor chat functions or similar communication services that are not open to all players but allow connectivity between a finite number of players who can decide themselves with whom to connect.

5. Third party data

Online gameplay services not only process data received or collected from the player directly. Information is also shared from,

or shared with, external third-party service providers. The majority of them are providers involved in the technical supply of the service, e.g. gaming platforms, data analytics companies and financial institutions that verify payment transactions. In addition, data may also be shared with administrative or judicial authorities to comply with a legal obligation, e.g. in connection with an investigation of fraud or intellectual property infringement, or to protect the rights and safety of the players. This category of data may also include data processed for the purpose of providing the player personalised advertisements or personalized content. In addition, information about the player may be shared as well with social networking sites or other video game publishers if he has chosen to link his account with these services. Sometimes data is shared with marketing companies directly. Targeted advertising requires an analysis of a player's personal data to detect characteristics or behavioural patterns with a view to make predictions. However, sharing data for the purpose of targeted advertising is not a common business model in the games industry and its importance is declining. Unlike in other media industries, refinancing takes place primarily through sales of games, in-game purchases as well as subscription models and fees for services.

III. Grounds for lawful data processing

The above-mentioned processing activities in video games must of course be carried out lawfully and should be based on the legal grounds in Art. 6 of the GDPR which apply on the same footing. Due to the direct contractual relationship between gameplay providers and players, most data is processed on the legal basis for processing that is necessary for the performance of a contract while other processing operations are justified by legitimate interests. Consent is usually only obtained if it is really necessary.

1. Processing necessary for the performance of a contract

A contract that provides for the supply and use of a video game product requires the provider to make the game available and ensure that it runs smoothly from a technical point of view.⁶ In order to fulfil these contractual obligations, device and network data must be collected so that the game can be played on the user's device. Account data must primarily be provided for billing purposes, but also to comply with the minor protection rules. Gameplay data is used to enable the player experience. Without the multiplayer mode or the location function in a location-based game like Pokémon Go, essential game functions are technically impossible. The detection of bugs, cheats, bots or trolls contributes to the smooth functioning of the game and is therefore covered by the contract.

In the case of communication and interaction data, a distinction must be made between the provision of a means of communication for planning and coordination between the players and the communication between the provider and the user. In both cases, the collection of communication data can be covered by the contract, for example, when communication is part of the gameplay or reporting mechanisms are integrated to ensure a

⁴ The JuSchG and many other laws explicitly require such reporting mechanisms. Comprehensive reporting tools are also discussed in the DAS.

⁵ The new Telecommunications Modernisation Act implemented the European Electronic Communications Code (Directive (EU) 2018/1972) which entered into force on 20 December 2018. Recital 17 explicitly mentions communication channels in online games as examples that do not fall under the concept of an "interpersonal communication service"; cf. also *Kollmann*, MMR 2021, 462.

⁶ With the Act Implementing the Directive on Certain Aspects concerning Contracts for the Supply of Digital Content and Digital Services, the main contractual terms and conformity requirements are explicitly listed in §§ 327b ff. BGB and, for example, also establishes new obligations regarding updates, § 327f BGB.

smooth experience.⁷ The transfer of personal data to third parties may also be considered as part of the contract, as far as it supports the technical provision of the gameplay or the billing process. However, where marketing activities have no relation to the gameplay or where toxic players are banned from the game, the processing will be based on other lawful grounds. All these processing operations are usually explained in detail in the privacy policy, and in the EULA (End User License Agreement) or the Account User Agreement.⁸

2. Legitimate interest

Legitimate interests play an important role in the lawful processing of personal data. Many publishers offer players individually tailored additional content. This may include special skins or equipment, new levels or expansion packs as well as comparable game titles from the same publisher. These services are not part of the contract and are acquired through in-game purchases as a separate legal transaction. They are, nevertheless, very popular. In this context, personal data is processed for the purpose of providing targeted marketing which is usually done by the company's own customer service or, in some cases, by a third-party provider. Such a form of direct marketing can constitute a legitimate interest, as set out in recital 47 of the GDPR. A balancing test must then be carried out between the legitimate interest of the publisher to „market“ his products – taking into account the circumstances of each individual case – and the potentially conflicting interests and legal position of the data subject. In particular, it must be determined what the data subject can objectively and reasonably expect. In other words, whether the processing of personal data for the purpose of direct marketing is considered typical in the specific segment of the social domain and therefore socially accepted or whether it is not typical and should be rejected. In the games industry, in-game purchases are very common and for most free-to-play games (F2P) they are the only revenue stream. In this respect, it must be assumed that offers for virtual items and expansion packs are socially accepted and therefore justified. Furthermore, while additional safeguards in relation to advertising and profiling are required to protect children (recital 38 GDPR), the provisions of Section 7 of the Unfair Competition Act (UWG) must be taken into account as well. This, however, does not lead to a different assessment in the case of providing direct advertising to existing customers.

3. Consent

Consent is required in all other situations where the above-mentioned legal grounds do not apply. It constitutes a catch-all justification in practice. In principle, consent must be obtained when personal data is processed for the provision of personalised advertising or personalised content, in games that operate via social networks or where the player's account is linked to such services. The same applies to the processing of special categories of personal data according to Art. 9 of the GDPR which are, how-

ever, only rarely collected. It is nevertheless conceivable that a future video game would, for instance, use the VR headset to collect health data. In case of tracking and profiling, consent is often used while other legal grounds can be invoked as well (Art. 22 (2) GDPR). In an online game, consent is usually obtained on the landing page of a company's consent management dashboard. Consent must be given prior to the collection of the personal data and never retrospectively. For PC and console games, consent is obtained during registration or when the game is launched for the first time. Apple's new App Tracking Transparency Framework (ATT) imposes a central and one-time consent request to allow tracking of a user on its platform.⁹ In order to avoid early abandonments and increase the so-called conversion rate¹⁰, consent can only be provided on the ATT framework after a tutorial has been run through. Consent must always be given explicitly and voluntarily, whereby the data subject must be sufficiently informed about all aspects of the processing operations and about his or her rights as a data subject. Consent can be withdrawn at any time in accordance with Art. 7 para. 3 of the GDPR. In the event of contract termination, withdrawal of consent is not necessary, as Sec. 327q (1) of the Civil Code (BGB) refers to the provisions of the GDPR. Sec. 327q (2) clarifies that a player can be refused the continued use of the service if he objects to the processing of his data or withdraws his consent.¹¹

Consent in the context of minors is a particular challenge. Pursuant to Article 8 (1), minors who have reached the age of 16 can effectively consent to the processing of their personal data without requiring the consent of the holder of parental responsibility. If the child is below 16, the lawfulness of the data processing is dependent on consent of the holder of parental responsibility. While many gameplay providers register the age of the player to comply with minor protection rules, technical protection measures (such as parental control tools) may also allow further verification to a certain extent. In this respect, the obligation under Article 8 (2) GDPR can be fulfilled by ensuring that consent was given by the child or by the holder of parental responsibility for the child. Finally, it should be noted that the transfer of profile and user data to third parties without consent is now considered an interaction risk in the Youth Protection Act (JuSchG) since the adoption of its amendment Sec. 10b (3) which was probably inserted to target in particular tracking data.

IV. Tracking

Tracking usually requires consent for both personal and non-personal data. So-called cookies are able to track the user behaviour in online and browser games and sometimes used for marketing purposes. A distinction must be made between first-party cookies („own“ cookies) and third-party cookies. First-party cookies are indispensable for the operation of the game and often provided through the browser or the app store for device recognition, for enabling the desired or acquired settings, for displaying the correct language version and for preventing mass registrations. They are also called functional cookies. Third party cookies, on the other hand, are cookies from authorised third party providers. They are often used to track a provider's webpage visits and views. They can be necessary for the detection of download problems or other software issues¹², for fraud prevention¹³ or for protection against spam¹⁴. Cookies from third-party providers are also used for marketing purposes. They are used in this context to detect „conversion events“, i.e. to detect a particularly high or low amount of app downloads, abandoned registrations, or purchases. In general, this information is aggregated or at least pseudonymised. However, tracking data also allows advertising networks and other advertising companies to display

⁷ According to the future ePrivacy Regulation, consent may be required if the communication channel connects a limited number of players who can decide for themselves with whom they connect.

⁸ For example, on the EA Origin gaming platform, available at: <http://tos.ea.com/egalapp/eula/DE/de/ORIGIN/>.

⁹ The background and impact of this new framework is discussed in detail by *Mitsching/Rauda* in this supplement.

¹⁰ The conversion rate (CRV) is the ratio of the number of website visitors in relation to the number of transactions, which in this case is the number of newly acquired players.

¹¹ The situation is different in California where the CCPA prohibits discrimination in the exercise of one's right to object.

¹² Crashlytics or Firebase are examples of third-party providers that are often used.

¹³ Third-party providers such as Kount, Riskified or Signifyd are often used.

¹⁴ Akismet, Captcha or Cleantalk, for example, are often used as third-party providers.

advertisements, to anonymously attribute marketing activities to specific marketing partners such as influencers or „Let’s Players“, and to optimise marketing efforts on the basis of conversion figures by avoiding retargeting of addressees and excluding those who have opted out. In addition to cookies, browser-based tracking data can also be collected via tracking links or log-in solutions such as Facebook Connect, Google Sign-In or Sign-In with Apple. On mobile platforms, tracking data is collected via partner modules in Adjust or AppsFlyer. However, some browsers¹⁵ no longer allow third-party cookies for marketing purposes. Third-party cookies, but not first-party ones, can also be blocked by Ad Blocker software.

The ECJ ruling on Planet 49¹⁶ made clear that the use of cookies – irrespective of whether personal data are processed – generally requires active and voluntary consent under the ePrivacy Directive. An exception applies when cookies are strictly necessary for a service requested by the user or for the sole purpose of carrying out the transmission of a communication (Art. 5(3) ePrivacy Directive). This is now formalized by the new Telecommunication Telemedia Data Protection Act (TDDSG) which will come into force together with the revised Telecommunications Act on 1 December 2021. According to Sec. 25 of the TDDSG, cookies are permitted without consent if they are absolutely necessary to provide a telecommunication service expressly requested by the user (functional cookies). In any case, a waiver of consent pursuant to Sec. 15 (3) TMG is no longer possible.¹⁷ Consent for tracking is usually obtained during the registration process of browser-based game or when a mobile game is played for the first time. Browser-based consent is often obtained via a cookie bar or a banner on the landing page. This is not possible on mobile platforms and usually done via the AppStore. In both cases, it must be ensured, according to recent case law, that consent cannot be skipped and that it can be freely given and with an affirmative action (no pre-ticked boxes).

V. Data Transfers

Video games companies transfer personal data of players to third parties for various reasons. Most commonly, data is transferred within a company or a group of companies to the department responsible for the respective processing, such as the accounting, legal or privacy department.¹⁸ Groups of companies typically aim to take advantage of synergy effects, especially in the area of customer acquisition or cross-marketing. In this context, newsletter data often plays a special role in the planning and implementation of marketing activities.¹⁹ Such data transfers usually take place in the context of commissioned processing, although this must be clearly separated from joint data processing operations. A particularly relevant problem today is the cross-border transfer of data to third countries such as the USA and the United Kingdom.

1. Commissioned data processing by video games companies

Video game companies, like any other companies, often commission a range of selected external service providers, such as data centres or platforms, for sending newsletters or for implementing payment solutions. Such service providers are also regularly used to assess the results of advertising campaigns or to assist in the prevention of fraudulent behaviour and breaches of the terms of service. According to a short paper of the data protection authority of the Federal Government and the Länder (*Data Protection Conference – DSK*), commissioned data processing within the meaning of Art. 28 GDPR exists in particular when it is necessary or possible for the data processor to access the personal data. If, for instance, the IP address of the user is shortened and anonymised and the personal reference of the IP

address is thus removed, commissioned processing would not exist due to the lack of a personal reference. Such an approach is certainly useful for billing and accounting purposes. Gameplay data is usually not transferred by video game companies as this type of data is almost regarded as a trade secret.

2. Joint data processing operations

Regarding video games on social networks such as Facebook Instant Games and Snap Games Platform, a distinction must be made between games that are only available and playable on the social network and games for which a player must have a user account on the social network. The ECJ²⁰ ruling that Facebook should be considered as a controller in situations where it processes personal data of its users and of the visitors of Facebook supported fan pages and that consequently joint controllership applies, can also be applied to video games on social media platforms. Accordingly, video game providers must conclude corresponding data processing agreements with the platform operators in addition to a legal notice, a privacy policy and the terms of use of the game. However, in view of the ECJ decisions in the Zeugen Jehovah²¹ and Fashion ID²² cases, it should also be pointed out that a clear line for joint responsibility has not been set out yet.²³

3. Data transfers to third countries

Where joint or commissioned data processing activities are carried out in the context of cross-border data transfers to third countries, an adequacy decision pursuant to Article 45 GDPR or other appropriate safeguards pursuant to Article 46 GDPR must be in place. Such an adequacy decision is now required for the United Kingdom as a consequence of Brexit and must be adopted before the end of the transition period on 1 July 2021. In this respect, it is possible that video game companies will have to use standard contractual clauses (SCC) or Binding Corporate Rules as a transitional measure.

The same already applies to the USA where due to the ECJ ruling in the Schrems II²⁴ case, the EU-US Privacy Shield is not a sufficient basis anymore for transfers of personal data. However, the vast majority of video game companies already make use of these SCCs and apply additional technical and organisational measures. On 4 June 2021, the EU Commission adopted new SCCs for the transfer of data to third countries.²⁵ The previous SCCs will be repealed after three months from the entry into force of the new set of clauses. A transitional period of 15 months will apply for contracts concluded before the date of repeal during which the data transfer can take place on the basis of the previous set of clauses.

¹⁵ For example, Firefox, Apple Safari and, from 2022 onwards, Chrome.

¹⁶ ECJ MMR 2019, 732 with note by Moos/Rothkegel – Planet49; BGH MMR 2020, 609 with note by Gierschmann – Cookie-Einwilligung II; on the requirements for cookie banners see also Haberer, MMR 2020, 810 and Sesing, MMR 2021, 547 – in this issue.

¹⁷ Excerpt. BGH MMR 2020, 609 with note by Gierschmann – Cookie Consent II.

¹⁸ In the case of a uniform corporate database, the principle of separation from Article 5 (1) (b) of the GDPR (“purpose limitation”) must be observed at all times.

¹⁹ Bodensiek/Hoffmann write in this supplement specifically about the handling of newsletter databases in groups of video games companies and the legal requirements for sending them to customers of other group companies, as well as the considerable problems that may arise in carrying out requests for deletion and opt-out.

²⁰ ECJ MMR 2018, 591 with note by Moos/Rothkegel – Facebook Fanpages.

²¹ ECJ ZD 2018, 469 with note by Hoeren – Jehovah’s Witnesses.

²² ECJ MMR 2019, 579 with note by Moos/Rothkegel = ZD 2019, 455 with note by Hanloser – Fashion ID.

²³ Lober/Klein write in detail about data protection in games on social networks such as Facebook, Snapchat & Co. in this supplement.

²⁴ ECJ MMR 2020, 597 with note by Hoeren = ZD 2020, 511 with note by Moos/Rothkegel – Schrems II.

²⁵ S. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

VI. Conclusion: Same same, but different

After three years since the GDPR came into force, video games companies have developed practicable and customer-friendly solutions for the protection of personal data that have largely proven their worth. Unlike in other media industries, the focus does not lie on tracking and targeting consumers for the provision of third-party advertising. Typical processing operations rather aim to improve the player experience and provide tailored gameplay offers. Such processing is usually covered by legitimate interests whereby cookies can be considered as functional and therefore not require consent. The GDPR provides for a Europe-wide legal harmonisation and is therefore of great added value for a sector that distributes its products throughout Europe.

However, the divergent interpretation of the harmonised standards is nevertheless problematic. This is clearly reflected in the supervisory structure of the legal framework.²⁶ In the application of the existing rules and the upcoming new law reforms, such as the ePrivacy Regulation and the Data Act, it will become clear whether the specific requirements and operating modes of the video games industry are understood and taken into account.

²⁶ This is not discussed further in this article but dealt with by Moos in detail in this supplement.

For a quick read ...

- There are many different types of data categories collected in video games, but fewer for the purpose to provide advertising than to support the player experience.
- Data processing is mostly carried out on the legal basis that it is necessary for the performance of a contract and partly also to pursue legitimate interests, while consent is rather the exception.
- Tracking and cookies are often used for cross-platform gameplay services and to improve the player experience, but usually not for targeted advertising by third parties.
- Data transfers to third countries are usually based on standard contractual clauses, in particular because the data has to be shared worldwide.



Jürgen Bänsch

is Director Policy & Public Affairs at the Interactive Software Federation of Europe (ISFE) – the Association representing the European Video Games Industry in Brussels.



Professor Dr Christian-Henner Hentsch, M.A., LL.M.

is Head of Law & Regulation at game – Association of the German Games Industry in Berlin, Professor of Copyright and Media Law at the Cologne Research Centre for Media Law at TH Köln and co-editor of MMR.

PATRICK MITSCHING / CHRISTIAN RAUDA

Turning point in tracking usage behavior through games apps

Significance of Apple's App Tracking Transparency Framework (ATT Framework) for Game Development Studios from a Data Protection Perspective

User and device data

This article addresses the categorization from a data protection law perspective of the App Tracking Transparency Framework („ATT Framework“) introduced in April 2021 on Apple devices from iOS 14.5. Although Apple is not a legislator and the ATT framework is not a law, ATT has de facto legal status due to global platform terms and conditions vis-à-vis game developer

studios and players. For the first time, an unavoidable mechanism is being created for a manufacturer's mobile devices to obtain permission from players for tracking beyond the game app in other apps and websites. This has far-reaching consequences, especially for the promotion and monetization of game apps that rely on tracking. **reading time: 18 minutes**

I. Introduction

Apple has shaken up the world of app development studios. In the operating systems iOS 6 to iOS 13, app developers had free access to the unique Identifier for Advertisers of the Apple device („IDFA“). An IDFA is a unique and globally valid identification number inherent in every Apple device, consisting of 32 characters (e.g. EA7583CD-A667-48BC-B806-42ECB2B48606). Users did have the option to change access by modifying the privacy settings. One could first reset or lock the IDFA. Since iOS 14, resetting has no longer been possible, but it was possible to manually block access to the IDFA completely by deactivating the menu item „Allow apps to request to track“. However, many users were not aware of this option. This meant that the majority of users could be tracked without any need for further action.

Apple has now restricted the possibility of tracking and has received a lot of praise from the data protection community for this, but has also faced a lot of criticism. Under the flag of data protection, Apple is pursuing its own economic interests.

II. App Tracking Transparency Framework

With the update of the iOS operating system to version 14.5 on 26th of April, 2021, the so-called App Tracking Transparency Framework („ATT Framework“) was introduced. Apple now requires app development companies to use the ATT framework if their app collects data about end users and shares it with other companies for the purpose of tracking across apps and websites. This merging regularly happens in two cases. Firstly, in cases when the app developer advertises their own app with a

digital advertising company (user acquisition). Or, secondly, if the app developer makes advertising space in their app available to advertising companies for a fee (ad sales). In both cases, the app developer and the advertising company exchange the IDFA of successfully recruited users (attribution). This enables clear measurement of and remuneration for advertising success. It also limits fraud. Otherwise, there would be a risk that the app developer would pay for the acquisition of fictitious users, i.e. users who were not brought to them by the advertising company (advertising fraud).

III. What does „Tracking“ mean for Apple

By „Tracking“, *Apple* refers to its linking of user or device data collected from other companies' apps, websites or offline properties for the purpose of targeted advertising or ad measurement. Tracking also refers to the sharing of user or device data with data brokers¹. *Apple* also gives examples of tracking, namely:

- Displaying targeted advertising in the app based on user data collected from apps and websites of other companies.
- Sharing device location data or email lists with a data broker.
- Sharing a list of emails, advertising IDs or other IDs with a third-party advertising network that uses this information to re-target these users in other developers' apps or find similar users.
- Placing a third-party software development kit (SDK) in the app which combines user data from the app with user data from other app developers' apps to target advertising or to measure advertising effectiveness, even where the SDK is not used for these purposes.

Tracking does not include when user or device data from the app is linked to third party data only on the user's device and is not sent from the device in a way that can identify the user or the device, or when a data broker with whom data is shared uses the data solely for fraud detection, fraud prevention or security purposes and solely on behalf of the app developer.

IV. Implementation of the ATT Framework

Technically, the implementation of the ATT framework requires that app development studios incorporate into their app a program code which is specified by Apple and which is uniform for all apps. This code leads to the display of a system dialogue (ATT prompt) when the app is started. This ATT prompt asks users to give permission to „allow the app to track their activity across other companies' apps and websites“. In addition, a description of the reason for tracking must be displayed by the app developer (usage-description string). The users of the app are free to give permission or not. *Apple* points out that the app may crash when users launch it for the first time if no usage-description string is implemented. After users have given or refused permission, the app stores their decision (tracking authorization status). In this respect, the app developer has only one „shot“ to obtain permission. This has led many app developers to wait until after the introduction of the ATT framework and not activate an ATT prompt at first.² If users of the app do not give their permission, the app developer cannot ask for permission again. Instead, users must actively grant permission to the app developer in the system settings. *Apple* prohibits app developers from circumventing the „one shot“ rule. For example, it is forbidden to show a separate window before the native ATT prompt where users can select „I'll decide later“ and thereby defer the decision. It is also not permitted to link the use of the app to the granting of permission (gating) or to make the granting of permission more attractive through incentives such as free services or discounts (incentivization).³

There are few discernible incentives for users to agree to tracking. Many users do not even realize that there is a difference be-

tween tracking on the internet and displaying advertisements. Withholding permission for tracking does not, of course, prevent advertising from being displayed to users. Without tracking, the advertisements displayed are just no longer tailored to the users' interests. This can lead, for example, to vegans being offered meat products or men being offered hygiene products for women. Hardly anyone realizes that tracking also has advantages for users. This means that many people will withhold permission. Historically, prior to the introduction of ATT in April 2021, approximately 90% of all IDFAs were freely available because few users disabled tracking in their system settings. Recent surveys since the ATT introduction in June 2021 indicate that the effective IDFA availability rate is settling at 15 to 20% or less depending on app category and geographic region.⁴ The consequences for app developers are high wastage in user acquisition and falling advertising revenues. The advantage of online advertising compared to out-of-home or television advertising, for example, is that the target group can be identified and addressed much more precisely. This minimizes wastage and increases the willingness of manufacturers and retailers to spend high prices on targeted advertising. The biggest advertising companies by far, *Facebook* and *Google*, claim that the revenues of advertising space providers – here: app developers – would decline by 50% (*Facebook's* estimate) and 52-64% (*Google's* estimate) without personalized advertising.⁵ These figures are also cited by German advertising associations in their current ATT cartel complaint against *Apple* before the *Federal Cartel Office (Bundeskartellamt)*.⁶ However, it should be noted that independent empirical studies forecast a much smaller decline in revenues, by only about 4%.⁷ Game development studios that can largely only offer in-game advertising which is not tailored to the interests of the user will therefore earn less advertising revenue.

V. Data protection classification

1. Classification of ATT permission as consent

It is disputed whether the „permission“ requested from the developer via the ATT framework is consent in the sense of data protection law. The question has relevance for serving ads to users on other devices and platforms, especially those outside Apple's digital ecosystem.

According to the consent theory, the requested permission may be consent within the meaning of Art. 6(1)(a) GDPR, which refers wholly to the app developer's authority to track.⁸ Accordingly, users attribute a legal quality to the ATT prompt and decide, with reference to the app developer, whether they agree to

¹ <https://developer.apple.com/app-store/user-privacy-and-data-use/>.

² <https://www.businessinsider.com/why-you-are-not-seeing-ios-145-privacy-pop-ups-2021-4/>; <https://www.fastcompany.com/90632354/ios-14-5-privacy-pop-up-requests-not-showing-up>.

³ See footnote no. 1.

⁴ Flurry: 15%, available at: <https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/>; Singular: 20%, available at: <https://www.singular.net/blog/ios-14-5-by-the-numbers-adoption-att-permission-ad-spend-trends-install-volume-impact-on-android-vs-ios/>.

⁵ Facebook: -50%, available at: <https://developers.facebook.com/blog/post/2020/06/18/value-of-personalized-ads-thriving-app-ecosystem/>; Google: -52-64%, available at: https://services.google.com/fh/files/misc/disabling_third-party_cookie_s_publisher_revenue.pdf.

⁶ *Pettinger*, Zwingt Apples Datenschutz Unternehmen in die Knie?, available at: <https://www.dr-datenschutz.de/zwingt-apples-datenschutz-unternehmen-in-die-knie/>.

⁷ *Marotta et al.*, Online Tracking and Publisher's Revenues: An Empirical Analysis, available at: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

⁸ *Obereck/Frank*, iOS 14.5 – Apple gibt Nutzern Wahlrecht bei App-Tracking, available at: <https://www.datenschutzkanzlei.de/ios-14-5-apple-gibt-nutzern-wahlrecht-bei-app-tracking/>; *Isaacson*, Apple iOS14 Changes: „Your App“ May No Longer Mean „Your Data“, available at: <https://www.adexchanger.com/data-driven-thinking/apple-ios14-changes-your-app-may-no-longer-mean-your-data-2/>.

tracking across all the devices and platforms on which the game is offered. This is supported by the fact that Apple, in its ATT guideline, attaches a very comprehensive meaning to the user's decision on permission or refusal of tracking, which abstractly refers to the „app“ as a universal product that can be used on different devices and platforms.⁹

The device-specific theory represents an opposing opinion. According to this perspective, the granting or refusal of permission is a mere device setting, which has no general legal quality and thus also has no legal effect vis-à-vis the app developer.¹⁰ For the user, the ATT prompt is simply a query regarding a system setting which is only valid for this one device. Accordingly, there is no consent as per the terms of the GDPR because the obligations to provide information under Art. 7 GDPR have not been fulfilled, as the ATT prompt cannot be linked to the privacy policy.¹¹ The users do not prohibit the app developer from tracking beyond the specific Apple device on which the setting is selected.

The matter of which opinion one follows will have far-reaching consequences in relation to games which can be played across many different devices and platforms (cross-platform games). Cross-platform games are characterized by the fact that they can be played on different end devices and operating systems. If you have been playing a mobile game on the train back from work, you can continue to play the same game seamlessly on your PC after you get home. If e. g. a user plays the cross-platform game „Forge of Empires“ on their iPhone, iPad and PC, the tracking permission may well fall apart. For the iPhone, for example, they refused tracking, for the iPad they accepted tracking and for the PC they were not asked about tracking at all because it does not use the iOS operating system and therefore the ATT framework does not apply there.

The device-specific theory is supported by the fact that users who give their response to the ATT prompt only have the specific device in mind which they are using at that moment. They do not give any thought as to whether this permission may have any effect on the use of the game on other devices or platforms. Any other view is impractical and constructs a legal will that the users do not have. However, the device-specific theory fails to grasp that the user decision does indeed have an inherent legal quality in relation to the device concerned: Users express their agreement or disagreement with tracking through their response to the ATT prompt. The query in the ATT prompt is made in deliberately simple and clear language, as required, among other things, by recital 58 GDPR. Users can easily read the privacy policy on the app's app store page before or during installation. In this respect, no excessive demands should be made of the content and scope of the ATT prompt – the prompt is clear and alerts the user sufficiently. A persuasive case can therefore be made that the device-specific theory should be modified to allow device-specific consent via the ATT prompt.

From a data protection point of view, the implementation of such a permission with the character of consent, before any tracking occurs, is desirable.

⁹ See footnote no. 1

¹⁰ Apple's ATT: Was es bedeutet, wenn kaum einer Tracking will, available at: <https://www.dr-datenschutz.de/apples-att-was-es-bedeutet-wenn-kaum-einer-tracking-will/>; *McChannel*, Be Cautious App Developers: ATT and GDPR are not the same, available at: <https://appgrowthsummit.com/be-cautious-app-developers-att-and-gdpr-are-not-the-same/>.

¹¹ See footnote no. 10

¹² *Koreng/Lachenmann*, Formularhandbuch Datenschutzrecht, 2018, F. I. 2. no. 7.

¹³ <https://support.google.com/admanager/answer/6280452?hl=en>.

¹⁴ *Weichert*, SVR 2014, 201 (204); *Hoffmann*, MMR 2013, 631 (634).

¹⁵ ECJMMR 2019, 732 with note by *Moos/Rothkegel* – Planet49.

¹⁶ ECJMMR 2019, 736 with note by *Moos/Rothkegel* – Planet49.

¹⁷ ECJMMR 2019, 736 with note by *Moos/Rothkegel* – Planet49.

2. Classification of IDFA as personal data under GDPR

The IDFA enables linking with further personal data through which a personal reference can be established, but not with data permanently assigned to the device.¹² In practice, the IDFA is very similar to a cookie in its function: A cookie placed in the browser, much like the IDFA placed in the iOS operating system, allows user behavior to be tracked. Just as a cookie logs the websites accessed by the user, and the entries made on them, the IDFA logs the apps and websites accessed by users and the actions performed therein. The only technical difference is that a cookie has to be manually integrated by the website provider into the source code of their website, whereas the IDFA is already present in the iOS device from the day of purchase. Ultimately, the data collected from a cookie and from an IDFA are traded on the same basis as other economic goods. A website or app provider that can provide tracking data on user and purchase behavior will receive significantly higher advertising revenue from advertisers than will a provider that cannot or will not provide tracking data. In the advertising industry, cookies and IDFAs are uniformly treated as „audience identifiers“, with cookies being relevant for the „web“ sector and IDFAs for the „non-web“ sector.¹³

However, there is still controversy over whether an IDFA represents personal data in the sense of the GDPR. Recital 30 GDPR states that „natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.“ This may „leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.“ At first, it was possible to reset or deactivate an IDFA and since iOS 13 it has been possible to switch it off (Limited Ad Tracking – LAT). However, if this is not done, there is a strong argument for considering an IDFA to be personal data.¹⁴

3. Classification of IDFA as protected information under the ePrivacy Directive

After the ECJ ruled in the Planet49¹⁵ case that consent is generally required for the use of cookies on websites, the question naturally arose of how this should be assessed for other tracking technologies. Essentially, an IDFA is to iOS mobile devices what cookies are to websites. Cookies were a source of controversy for years because they enabled the tracking of users as they surfed from website to website, which in turn enabled profiling and thus targeted advertising. On mobile devices, advertising IDs (like IDFA) practically completely replace cookies, which do not exist there for technical reasons, and enable the tracking of users during interaction in the various apps and websites, meaning that profiling and targeted advertising are also possible on these devices. As a rule of thumb, one always need consent when using such technologies if this is provided for under the ePrivacy Directive (ePrivacy Directive).

Art. 5(3) ePrivacy Directive deals with storing „the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment“. It must be ensured that users are made aware that they have the option to refuse this storage. In the Planet49 decision, the ECJ makes it clear that the consent requirement in Art. 5(3) sentence 1 ePrivacy Directive applies regardless of whether the information stored in a cookie is personal or anonymous data. Article 5(2) of the ePrivacy Directive also does not require that the storage of or access to personal data must relate to personal data.¹⁶ It is about the protection of all information stored in users' end devices, without differentiating between personal and other information.¹⁷

Since the IDFA is stored in the user's device, consent is therefore required. In this context, it should also be noted that on 20th of May, 2021, the *Bundestag* passed the draft of a law regulating data protection and privacy in telecommunications and telemedia (TTDSG). Section 25 TTDSG-E is intended to implement Art. 5 (3) ePrivacy Directive. According to this provision, the storage of information in the end-user's terminal equipment or access to information already stored in the terminal equipment should only be permitted if the end-user has consented on the basis of clear and comprehensive information. The provision is directly based on the wording of the European requirements.¹⁸ According to the explanatory memorandum of the government draft, Section 25 TTDSG-E only applies to non-personal data; with regard to personal data, the GDPR is the governing body.

VI. Criticism of the ATT Framework

The introduction of *Apple's* ATT framework was strongly and publicly criticized by *Facebook* and by advertising associations, inter alia, who argued that *Apple* was forcing app developers to switch from advertising to subscription models and in-app purchases, on which *Apple* makes a profit. In France, the advertising associations lodged a complaint with the anti-trust authority, but it was unsuccessful.¹⁹ In Germany, the advertising associations also filed a complaint with the Federal Cartel Office, which has not yet been decided at the time of writing.²⁰ *Apple* charges a fee of 30% of the transaction volume on all subscriptions and in-app purchases made in the App Store in a B2C relationship, with only few exceptions. In contrast, *Apple* does not profit from ad-financed apps, as the advertising remuneration is handled in a B2B relationship between app developer and advertising provider outside the app store.²¹ In addition, *Apple* is accused of wanting to sell more advertising space in the search results lists in the App Store, following *Google's* successful sale of advertising space next to the search results in Google Search.²² *Apple* is therefore allegedly not concerned with data protection at its core, but with increasing its own revenues and expanding its control over app developers.

Apple has greatly expanded its own advertising space in the App Store in parallel with the introduction of ATT.²³ In its App Store, *Apple* processes the first-party data collected in its own iOS ecosystem for advertising slots that third parties can book. Although it is not possible to target individual users, it is possible to target cohorts of 5,000 or more people where the individuals have similar characteristics.²⁴ Thus, ultimately, individual tracking will be replaced by the new cohort tracking. Even more sophisticated approaches are AI-based analysis of user behavior by means of „Differential Privacy“ and „Federated Learning“, which are used for example in the personalization of *Apple's* voice assistant Siri.²⁵ It should be noted, however, that such cohort tracking is also subject to the GDPR so long as data can be traced back to individual persons in this context. Since *Apple* does not have to share this treasure trove of data with anyone, it is particularly valuable. So-called „first-party“ tracking is privileged as opposed to „third-party tracking“.²⁶ For this reason, *Schwartmann* called *Apple* „a self-appointed and self-interested tax collector“.²⁷

VII. Conclusion

Game development studios need to innovate in their approach to user acquisition and ad sales. The trend is no longer to record the behavior of individual users, but to collect aggregated data at the level of groups of users with common characteristics (cohorts). Moreover, we should expect a move away from tracking based on deterministic markers such as advertising IDs and towards assumptions based on probabilistic markers such as device type, time of use and advertising context. In parallel to these

processes, the value of first-party data will increase for game development studios and advertising companies, as third-party data can no longer be collected and exchanged at will due to a lack of tracking consent. This will lead to increased vertical integration of game development studios and advertisers to build a shared inventory of first-party data. Further developments will also shed light on how dependent game development studios and the advertising industry really are on tracking individual users.

For a quick read ...

- By „Tracking“, *Apple* refers to the linking of user or device data collected from other companies' apps, websites or offline properties for the purpose of targeted advertising or ad measurement.
- The app developer must integrate a program code (App Tracking Transparency Framework – ATT Framework) into their app which is specified by *Apple* and is uniform for all apps. It is through this framework that the user's permission is requested for tracking. The effective tracking permission rate for game apps is now only around 15-20%. The consequences for game developers are high wastage in user acquisition and falling advertising revenues.
- The granting of permission is a consent related to the specific *Apple* device. However, it does not fulfil the requirements of a general consent valid for all devices and platforms vis-à-vis the game developer studio. This distinction is important for cross-platform games. Since the IDFA is stored in the user's device, consent is therefore required as per Art. 5 (3) ePrivacy Directive.
- Game development studios need to innovate in their approach to user acquisition and ad sales. The trend is no longer to record the behavior of individual users, but to collect aggregated data at the level of groups of users with common characteristics (cohorts). In addition, the importance of probabilistic data and first-party data is increasing.



Patrick Mitsching, LL.M. (Durham), M.A. (London), is Team Lead of the Legal Department at InnoGames GmbH in Hamburg.



RA Dr. Christian Rauda is board-certified specialist for information technology law, copyright and media law and intellectual property law. He is a partner in the media law firm GRAEF Rechtsanwälte (Hamburg/Berlin) as well as a lecturer at Bucerius Law School and Hochschule für Technik und Wirtschaft Berlin.

¹⁸ *Schwartmann/Benedikt/Reif*, MMR 2021, 99.

¹⁹ <https://www.autoritedelaconurrence.fr/en/press-release/targeted-advertising-g-apples-implementation-att-solicitation-autorite-does-not-issue>.

²⁰ <https://zaw.de/missbrauchsbeschwerde-der-medien-und-werbewirtschaft-gen-apple-beim-bundeskartellamt/>.

²¹ See footnote no. 120.

²² See footnote no. 20.

²³ <https://9to5mac.com/2021/05/04/apple-emails-search-ads-app-store/>.

²⁴ <https://searchads.apple.com/help/advanced/0021-set-campaign-refinements/>.

²⁵ *Hao*, How *Apple* personalizes Siri without hovering up your data, available at: <https://www.technologyreview.com/2019/12/11/131629/apple-ai-personalizes-siri-federated-learning/>; *Ippolito*, AI Differential Privacy and Federated Learning, <https://towardsdatascience.com/ai-differential-privacy-and-federated-learning-523146d46b85/>; <https://machinelearning.apple.com/research/learning-with-privacy-at-scale>.

²⁶ In principle, this is also the view of the *Data Protection Conference*, available at: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmng.pdf, S. 17.

²⁷ FAZ of 10th of May, 2021, p. 18.

Group Newsletters – Not a no-brainer!

Practice-oriented Examination of Handling Newsletter Databases

Newsletter Marketing

The article deals with the particular legal and practical problems of distributing a newsletter – from the beginning of the newsletter subscription to its end. The different types and forms of newsletters are examined and then given a legal classification. The article focuses, *inter alia*, on the usual problems with newsletter marketing in corporate groups, which often strive to optimize cross-marketing effects and create uniform

technical structures. After all, the games industry is constantly changing; corporate takeovers are a daily reality. This also gives rise to problems – e.g. with the integration of existing databases into the group structure after a company purchase. The problems arising – in particular from the field of competition law as well as data protection law – are examined primarily from a practical point of view. **reading time: 21 minutes**

I. Addressing customers via the Internet

The Internet is generally regarded – and rightly so – as a breakthrough invention. In particular, the Internet makes it possible to address customers directly by e-mail, without incurring the otherwise typical costs and time expenditures of printing and shipping. It is also technically simple to track and react to newsletter that has been sent out.

It stands to reason that newsletters – also due to how commonplace they are – are no longer as effective as they were a few years ago. Since the introduction of the GDPR, which was brought to popular attention by the media, consumers have also become significantly more sensitive to data protection. Nevertheless, the newsletter still enjoys great popularity in most companies as a popular instrument of customer loyalty and acquisition. Companies from almost all industries use the newsletter to address customers and highlight their product range.

In the effort of companies to address the largest possible number of customers with as much news as possible by newsletter, it should definitely not be neglected to carefully observe the necessary legal framework, in particular the data protection requirements. Special legal issues arise if the newsletter distribution is to be organized within a group of companies or if newsletter stocks are also to be used for products of other group companies.

II. Different types of newsletters

As is commonly known, not all newsletters are the same. There are different types of newsletters – in terms of the content, but also the sender – and thus no uniform and generally valid legal basis for sending them. In essence, there are product newsletters, company newsletters, and – in the case of corporations – group newsletters.

1. Product newsletter

The standard scenario for a product newsletter is that a customer has purchased a product and has either expressly consented to being sent a newsletter regarding the product (or other explicitly named products), or that the company as part of obtaining the e-mail address has called attention to the distribution of the newsletter and the possibility of objection without additional transmission costs. In the first case, the permissibility of sending the newsletter is based on § 7(2) no. 3 of the German Unfair Competition Act (UWG), Art. 6(1)(a) GDPR, whereas the second case has its legal basis in § 7(3) UWG, Art. 6(1)(f) GDPR.

The most common errors are found in the case of § 7(3) UWG that the requirements of its numbers 1 to 4 are usually not cu-

mulatively present, but rather the reference under no. 4 is usually missing or is not verifiably documented. Even if all conditions are met, § 7(3) no.2 UWG prohibits product newsletters from being used to promote group companies or their products.

Even in the case of express consent to receive a newsletter for a specific or similar product, group-wide cross-marketing is generally excluded. When interpreting the customer's consent, not only the general rules of interpretation according to §§ 133, 157 of the German Civil Code (BGB) must be observed, but also – naturally – the principle of purpose limitation in data protection law.

The principle of purpose limitation in regard of a consent derives from the tenet of purpose limitation in Art. 5(1)(b) GDPR. Pursuant thereto, personal data may only be collected for – previously – specified, explicit, and legitimate purposes. This does not mean that the data may be further processed in a manner compatible with said purposes. The purpose defines why certain personal data is collected and processed. When exploring the purpose limitation according to the GDPR, the following aspects must be considered:

- Prior to collection and processing, the purpose must be specified
- The purpose must be explicit and have a legal basis (cf. Art. 6 GDPR)
- In the event of a change in purpose – i.e. if the personal data is processed elsewhere – a new legal basis must be established pursuant to Art. 6 GDPR

Insofar as the customer has provided its consent to a newsletter being sent by a specific company for a specific or similar product, this consent may not be subsequently extended to group companies. Increased transparency requirements must also be observed concerning the issue of which other products may be advertised. In this case, the declaration of consent must be clearly stated (i.e. products or product groups) so that the customer can also understand the scope of his consent. The *German Federal Court of Justice (BGH)* had recently also referred to the requirements of §§ 305 et seq. BGB regarding the provisions on general terms and conditions – in particular,¹ the transparency requirement – since the declaration of consent is usually pre-formulated by the advertising company and therefore considered general terms and conditions.

Not only the consent itself can lead to a limitation of permissible advertising; other laws may also result in restrictions. In the games industry, the German Interstate Treaty on the Protection of Minors in the Media (JMStV) should be specifically mentioned here. Advertising for offers that potentially affect children and young people in their development or to harm their interests

¹ BGH ZD 2017, 327 with approving notes by Eckhardt.

must be sent separately from other advertising (§ 6, paras. 3 and 4 JMStV),² especially if it is known that the recipient is not an adult. It should also be pointed out that in both cases the customer must be given the opportunity to unsubscribe from the newsletter at any time. For the first case, this follows from the wording of § 7(3)(4) UWG and Art. 21(1) GDPR, whereas for the second case the revocability is based on the nature of the consent as revocable consent under the UWG³ as well as from Art. 7(3) GDPR. In both cases, the newsletter may be sent until receipt of the revocation, as the act of revoking consent only has effect for the future.⁴

Even if not required by law, it is recommended to carry out the „double opt-in procedure“ for validating the e-mail address as proof of consent or the lawful conclusion of the purchase⁵. If several declarations are simultaneously made – e.g. registration of a customer account and registration for one or more newsletters – it is sufficient to send a single confirmation e-mail for the double opt-in. Since the double opt-in e-mail only serves to verify the access authorization to the specified e-mail account and does not repeat the legally binding declaration, this also does not entail any potentially inadmissible connection of several declarations. After all, sending only one confirmation email is also in the interests of the customer, who does not want to verify his e-mail address every time, if he has already done so.

2. Company newsletter

A company newsletter basically refers to information about a specific company and its products. In this sense, the content framework for a company newsletter is invariably broader than that of a product newsletter, which is always limited to a specific product or similar products. In order to satisfy the requirements of case law on the transparency requirement⁶, however, a general consent such as „for any products“ may not be sufficient.⁷ Rather, the scope of the consent must be at least comprehensibly outlined – e.g. „and other print products.“⁸ The company newsletter can also be limited to information about the company and its development without reference to products. In this sense, the sole legal basis of relevance here is the consent in accordance with § 7(2) no.3 UWG, Art. 6(1)(a) GDPR.

3. Group newsletter

In the case of a Group newsletter, there can be two different thrusts: On the one hand, either all of the group companies should be granted the right to distribute the newsletter or one company should be granted the right to distribute the newsletter with regard to all products and services of its group. In both cases, the effectiveness of the consents is based on § 7(2) no.3 UWG and Art. 6(1)(a), Art. 7 GDPR.

Such consent to a group newsletter is again limited by the transparency requirement. As the German Federal Court of Justice has stated on multiple occasions,⁹ the declaration of consent must not only be transparent with regard to the products that may be advertised; the transparency requirement also applies with regard to the parties performing the dispatch, to whom authorization is to be given. A vague reference to group companies not specified in greater detail does not meet these requirements. However, even the naming of a very large number of companies (e.g. 20 companies) may no longer be transparent for the consumer. In this respect, it can only be advised to also focus on certain companies and their products in the group newsletter. The *Higher Regional Court of Frankfurt am Main* has ruled that it is permissible to name eight group companies.¹⁰ Furthermore, it remains applicable that as concerns the consent for the products and services, there must be a thematic restriction due to the transparency requirement.

III. Distribution by third parties

Within corporate groups, there is generally a department responsible for group-wide newsletter distribution or at least for coordinated marketing. Not all group companies distribute the newsletters themselves; it would not be convenient to do so. The following points need to be clearly communicated to the department responsible for group-wide newsletter distribution and kept up to date.

The distribution of a newsletter to Company A may also transpire via Company B: The precondition for such is that Company A may legally send the newsletter in accordance with the above-mentioned criteria and that a corresponding data processing agreement in accordance with Art. 28(3) GDPR exists between Company A („controller“) and Company B („processor“). In this case, no special consent is required from the customer.

A contract for the processing of data on behalf of the controller is not obsolete even if the customer in question has given its consent to receive newsletters from several group companies (including Company B): Such consent would authorize Company B to send a newsletter on its own behalf. To the extent, however, that this occurs on behalf of Company A, Company A remains the controller and thus all consent requirements must be met vis-à-vis Company A. This circumstance remains true even if this is simultaneously available for Company B on its own behalf as the controller.

Finally, the „small group privilege“ mentioned in recital 48 of the GDPR cannot replace such a data processing agreement: Recital 48 states that it is conceivable that affiliated companies may transfer personal data to other affiliated companies as the controller for purely internal administrative purposes on the basis of legitimate interests pursuant to Art. 6(1)(f) GDPR.¹¹ Classic examples of this are an institutional human resource department or accounting.¹² However, the present case is not about internal administrative measures, but about obvious external product advertisement. Application of the small group privilege would excessively extend the purpose limitation of the consent.

In these cases, the transparency requirement pursuant to Art. § 6(1) of the German Telemedia Act (TMG) applies, which is explicitly referenced in § 7(2)(4b) UWG: Pursuant thereto, the identity of the responsible sender (not the service provider) must be easily recognizable, immediately accessible, and always available from the newsletter.¹³ It is not prohibited to name the service provider, insofar as the responsible sender remains clearly recognizable, practicable e.g. via distribution by Group Company B on behalf of Group Company A. In principle, a link to a website with the legal information is sufficient, the reproduction of a company logo is not sufficient.¹⁴

² Beck'scher Kommentar zum Rundfunkrecht/*Ladeur*, 4. Aufl. 2018, JMStV § 6 recitals 24-25.

³ Fezer/Büscher/Obergfell/*Mankowski*, UWG, Komm., 3. Aufl. 2016, § 7 recitals 151, 152

⁴ *Gola*, in: *Gola, DS-GVO*, 2. Aufl. 2018, Art. 7 recitals 54-58

⁵ Spindler/Schuster/*Micklitz/Schirmbacher*, Recht der elektronischen Medien, 4. Aufl. 2019, UWG § 7 recitals 130-137, with extensive further references.

⁶ *BGH ZD* 2017, 327 with approving notes by *Eckhardt*.

⁷ *Mankowski* (see footnote 3), recital 137a.

⁸ *Koreng/Lachenmann*, Formularhdb. Datenschutzrecht, 2018, 2. recital 5.

⁹ *BGH MMR* 2013, 380 with approving notes by *Eckhardt*; *BGH ZD* 2017, 327 with approving notes by *Eckhardt*.

¹⁰ *OLG Frankfurt/M.* ZD 2019, 507 with approving notes by *Eckhardt*.

¹¹ *Nickel*, ZD 2021, 140 (143).

¹² *Laue*, in: *Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 1 recital 46.

¹³ *Sesing*, in: BeckOK IT-Recht, As of: September 1, 2020, TMG § 6 recitals 23-25.

¹⁴ *Spindler/Schmitz/Spindler*, TMG, 2. Aufl. 2018, § 6 recitals 21, 22.

Interim conclusion

There is no „group privilege“ in terms of group-wide use of address and other customer data for the purpose of distributing the newsletter. The „small group privilege“ is argumentatively defensible but does not thus justify access to address data of another group company for its own purposes, since the small group privilege can only apply to „internal administrative purposes.“ That said, distributing the newsletter is neither an „internal“ matter nor an administrative purpose; instead, it is relevant as advertisement.

IV. Companies added to the corporate group

If a corporate group acquires a company via a takeover of company shares, various elements must also be taken into account in regard to an existing group newsletter. In principle, the acquisition of a company in the form of the takeover of the company shares or merger is not an objectionable scenario under data protection law (compared to, for example, asset purchase), since the legal entity is retained – and thus any consents previously obtained in its favor remain valid.

In such cases, of course, the acquiring company should have checked – if possible, as part of already performed due diligence – whether the consent has been legally obtained or whether the requirements in accordance with § 7(3) UWG have been met and documented. In practice, a newsletter database can only be used without risk if the legal requirements have been demonstrably documented in order to provide proof of consent in the event of an alleged violation, in particular by documenting the double opt-in procedure.¹⁵

However, even if the audit did not reveal any legal abnormalities, the group now faces the problem that the consents purchased as part of the company acquisition only relate to receiving a newsletter from the acquired company. Here, the following obstacle emerges: The „old companies“ in the group cannot simply include the „newcomer“ in their newsletter communication – and the newly acquired company cannot simply integrate product advertising of the old companies into its newsletter. Naturally, this obstacle only applies to existing customers – in this respect, in cases of company acquisition, it is recommended that the new company adapt and expand the consent texts regarding distribution of the newsletter in a timely manner; however, the same is advised prior to the acquisition for the companies already existing in the group.

In practice, incentivizing customers to accept extended newsletter consent – e.g. by participating in a competition or offering special items/gaming items – has proven to be particularly effective. Such incentive systems are also not prohibited by any prohibition on bundling, as long as the explanatory content displayed to the consumer corresponds to the transparency requirements,¹⁶ even though the *Higher Regional Court of Frankfurt am Main* recently even considered a consent to be effective, although the business areas of the group companies were not fur-

ther defined.¹⁷ Rather, the *Higher Regional Court of Frankfurt am Main* stated that the consent should then be understood to refer only to the express business areas of the head company and this does not lead to intrinsic invalidity.

V. Use of external service providers for distribution

1. To be considered: multi-client capability

In the majority of cases, there is an external service provider that organizes and performs the distribution of the newsletter for the group companies. These providers specialize in sending and tracking newsletter distributions. The recipient databases are usually kept on a computer system of the service provider, and the service provider regularly organizes the double opt-in during newsletter registration.

As there is not usually a direct connection between the customer databases of the company and the database of the service provider, they are self-sufficient databases, which is already required by the separation rule.¹⁸

In this constellation, the requirements pursuant to Art. § 28(3) GDPR stipulate that a data processing agreement must be concluded between the controller and the service provider. In the particular case of group newsletters, it must be ensured that the controller here is always the respective distributor of the newsletter and that all group companies involved in the consent must conclude an order processing agreement. Theoretically, this is also conceivable for all companies in a single document, provided that care is taken to ensure that the legal representation of each company is assured. Against the background of the legal independence of the companies, however, it is recommended to conclude individual contracts, even if payment for such may be made centrally.

Before selecting an external service provider, it should be carefully checked whether the provider is able to organize the data of the consumer – i.e. at least the relevant e-mail address, but also the documentation and the material scope of the consent given by the customer – separately from the data of customers and other group companies, in accordance with the requirements of the separation rule under the GDPR. The „multi-client capability“ is primarily intended to prevent data collected for a predefined purpose from being mixed with data collected for another purpose.¹⁹ This ensures that the purpose limitation is also maintained in relation to each individual group company.²⁰ In principle, it is advisable for compliance reasons to examine the proposed data processing agreement in greater detail with regard to the technical and organizational measures.

2. Service providers in a non-member state: new clauses, new chances?

Insofar as the service provider has its registered office outside the European Union and there is no adequacy decision in accordance with Art. 45 GDPR, it must also be examined to what extent the provider complies with the standard clauses of the *EU Commission* under Art. 28, paras. 6, 7 GDPR. The other exceptions possible under Art. 46(2) GDPR are irrelevant in practice. It should be noted that on June 4, 2021 the *EU Commission* published a new set of standard clauses, which should be used effectively immediately.²¹ Old contracts using the old standard clauses may still be concluded during a transition period of 18 months in accordance with recital 24 of Implementing Decision (EU) 2021/914. However, it should be noted that the sole use of the old (as well as the new) standard clauses against the background of the Schrems II decision of the *European Court of Justice (ECJ)*²² – especially with regard to the United States – today

¹⁵ Auer-Reinsdorff/Conrad, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, recitals 129-136.

¹⁶ Gola (see footnote 4), recital 31.

¹⁷ OLG Frankfurt/M. ZD 2019, 507 with approving notes by Eckhardt.

¹⁸ Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Part XII. Sec. 2 E.VIII. recital 92.

¹⁹ Jandt/Steidle, Datenschutz im Internet, 1. Aufl. 2018, A.II.1.d)bb) recital 42.

²⁰ DSK, Orientierungshilfe Mandantenfähigkeit.

²¹ Cf. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de.

²² EuGH MMR 2020, 597 with approving notes by Hoeren = ZD 2020, 511 with approving notes by Moos/Rothkegel – Schrems II.

can no longer be considered sufficient. Rather, under the Schrems II decision by the ECJ, the standard clauses must be supplemented by appropriate provisions compensating for the risk of non-Member states violating the rights of the data subject.²³ In this respect, it is now up to each company individually to assess whether and, if so, which additional guarantees are necessary or sufficient in the destination country. Since there are no clear pre-defined criteria for this, the risk currently lies solely with the company exporting the data. In the meanwhile, *Microsoft*, *Google* and other providers already offer such additional guarantees, but it is questionable whether these are sufficient according to the standards of the ECJ. The *European Data Protection Board (EDPB)* itself assumes that it is not contractually possible to provide compensation for the risks of state intervention.²⁴ If so, the ECJ would have enticed all users into a veritable trap with its requirements. From a practical point of view, the recommendation remains to ensure that additional guarantees – possibly also of a technical nature – are offered, since otherwise, at least in the case of the USA, no permissible export of data can be assumed.

VI. Unsubscribe please – but from what exactly?

Even if it may be difficult to understand at first, the effective implementation of deletion requests can be quite complicated, especially with a group-wide newsletter solution. The problem begins with the question of what is to be regarded as a request for deletion for a newsletter subscription and ends with how data can be removed simultaneously and also in good time from a large number of databases that are fundamentally independent of one another.

1. Account termination

Game publishers and distribution platforms typically provide customers with the possibility to create a customer account („Account“). This Account often serves both as a customer account for purchases or for social media offers such as forums, as well as authentication for downloading purchased games or logging in for one or more online games. This typically entails creating a general customer account („Platform Account“), which then contains further sub-accounts („Gaming Accounts“). Legally, these are separate contractual relationships – a contractual relationship for the use of the platform and a separate contractual relationship for the use of the specific game.

In fact, it is often the case that in groups of gaming companies the platform operation is centrally maintained with one of the group companies, while the other companies offer their services on said platform in their own name and for their own account. For this reason, it is quite possible that the platform account is concluded with Company A, but the gaming account with Company B and/or Company C.

If a customer terminates „his account,“ this gives rise to the question of whether this also includes the unsubscribing from a newsletter. In principle, the declaration of the customer must be interpreted according to §§ 133, 157 BGB.

a) Gaming account

If the customer terminates a gaming account, it should be undisputed that said termination does not extend to any company or group newsletter that the customer had previously ordered. With the termination of a specific game, the customer does not specifically make clear that he is no longer interested in information about the company or the group.

However, even with regard to the product newsletter, it does not clearly follow from the termination of a gaming account that the

customer is no longer interested in the product or similar products. Thus, the possibility cannot be precluded that the customer only wants to take a break from playing but wants to be further informed in the event that he wishes to resume playing again. Especially when terminating a subscription, which can be subsequently resumed, there is no recognizable intent to terminate a newsletter registration. It is at least conceivable that a customer who terminates a gaming account and also requests the deletion of his gaming data is no longer interested in a pure product newsletter.

Some data protection authorities see the deletion request as a clear indication that the customer also wants to be removed from the product newsletter. This is absolutely understandable if the termination is accompanied by a general request for deletion of all personal data. If, on the other hand, the customer terminates only one of several gaming accounts with Company B or if only one subscription is terminated, which can be resumed at any time, there are no indicators that the customer is no longer interested in corresponding product information.

b) Company account

If the customer terminates his account for all offers of a company or for the entire platform – i.e. a termination, which may also include several gaming accounts – the interpretation is quite difficult, since he is thus indicating an absence of interest in the offer. However, if a game can be continued later by a new conclusion of an account, it is not clear whether there really is no fundamental interest anymore or merely a temporary lack of interest in use, but that there is still an interest in receiving information.

While the safest solution is the deletion from the company newsletter, this does not correspond to the company's interests and probably does not necessarily reflect the customer's interests. For this reason, it has therefore proven to be quite practicable to notify customers submitting a notice of termination – before concluding a termination (or if this was done by e-mail: as part of confirmation of receipt) – that they can manage their newsletter subscriptions independently and forward them to a website, where he can manually unsubscribe from any newsletter subscriptions they may have; this can be done in the form of standard consent manager systems (CMS). Against the background of the large number of declarations of intent required for interpretation – often groups of gaming companies have multiple current accounts in the tens to hundreds of millions – such a solution should be in the interests of all parties, insofar as a written termination was not absolutely clear in the individual case. Such a technical solution also corresponds to the requirement of „Privacy by Design“ within the meaning of Art. 25 GDPR.

This solution also makes it possible to get a handle on the biggest technical problem in these termination cases. As already explained, the newsletter databases are usually outsourced to external service providers, but at least to a central location within the corporate network. These newsletter databases are usually not connected to the companies' account databases. This means that the deletion of an account or the account data does not usually have an effect on the newsletter databases. In fact, it is usually not even clear from the account database whether the customer has ever ordered a newsletter or not.

If the intention is also to unsubscribe from a newsletter, it must be ensured that a deletion also takes place in the separate database. It becomes even more complex if separate newsletter da-

²³ *Schwartmann/Burkhardt*, ZD 2021, 235; *Heinzke*, GRUR-Prax 2020, 436.

²⁴ *EDPB*, Recommendations 01/2020, recital 48.

databases exist for several products – not to mention for multiple companies. Of course, this can be ensured by a customer service professional manually comparing databases, but this would hardly be practical. In this sense, a CMS – mentioned above – is advisable. However, this can only be realistically implemented if the respective newsletter service providers also provide interfaces that enable such management. Here it is advisable to address these requirements as part of the procurement process and then to implement them conceptually with the provider.

2. Unsubscribing from newsletters

If the customer uses a link or a button to unsubscribe from a newsletter (e.g. in the footer of a newsletter), it should be assumed that the customer only wants to unsubscribe from the specific newsletter. There is no obligation to direct the customer to a corresponding consent manager for other newsletters or even to provide him with said option. A company only needs to make available options for unsubscribing in the places required by law but does not have to force said options on the customer.

3. Data deletion requests

It is equally clear how to handle a data deletion request. If a customer wishes to delete all data that can be deleted (unless there exists a reason for not doing so pursuant to Art. 17(3) GDPR), this also includes any newsletter subscriptions. Since the request for deletion simultaneously indicates the revocation of consent to receive the newsletter in accordance with both the UWG and the GDPR, the provider must also ensure – upon receipt of such – that further newsletter distribution no longer takes place. The revocation takes effect immediately,²⁵ such that the effectiveness of any „implementation period“ agreed, for example, in the GTC, is at least questionable. A concept based on a manual implementation of such deletion requests should therefore be fundamentally problematic, since the absence of consent has immediate effect, whereas in the case of the deletion obligation this can be performed without undue delay in accordance with

²⁵ Ehmman/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, recital 92; Fezer/Büscher/Obergfell (see footnote 3), recital 152.

²⁶ Ehmman/Selmayr (see footnote 26), recital 40.

Art. 17(1) GDPR,²⁶ defined under Art. 12(3) GDPR as being limited to one month at most. It is thus not likely feasible to work without an automated solution. If the declaration, however, is not unambiguous, the recipient thereof must make at least one further inquiry – e.g. via the aforementioned consent manager.

Such a solution should be planned as part of a data deletion concept and implemented throughout the company in order to make it secure and practicable to distribute and unsubscribe from newsletters.

For a quick read ...

- The newsletter distribution should be organized and maintained – also and especially within the group – internally but also externally (service providers) from a single source.
- When distributing the newsletter, external service providers must be checked before concluding the contract – in particular with regard to their multi-client capability but also with regard to their country of origin.
- Even in the case of the customer having provided comprehensive consent to a group newsletter, data processing agreements must be concluded within the group on a regular basis.
- Technical solutions must take account of the considerable requirements of the handling of large customer databases, but also of the many different databases within the meaning of „Privacy by Design.“



Kai Bodensiek

is an attorney and partner in the Berlin office of Brehm & v. Moers Rechtsanwälte Partnerschaftsgesellschaft mbB.



David Julian Hoffmann

is Head of AdTech Legal and Group Data Protection at gamigo AG in Hamburg.

ANDREAS LOBER / SUSANNE KLEIN

Privacy in Multiplayer Games and Games on Social Networks

Special games – specific requirements: Global data transfers, semi-automated decision making and complex responsibilities

International Data Transfer

The popularity and success of computer games keep on growing constantly. This is especially true for so-called multiplayer games and games on the major social networks. What both have in common is that the player regularly does not remain alone, but either shares the gaming experience with others or can enter into direct competition with other players. In addition, games on social networks offer the advantage that even when not playing with friends from the network, registering for the game is particularly easy and convenient because the

existing user account can regularly be used for this purpose. In all these constellations, considerable amounts of personal data are processed. The related data protection issues concern the relevant legal bases, responsibilities, data subjects' rights and, last but not least, international data transfer because it is often the global gaming experience that is particularly appealing to players. This article focuses on the particularities in terms of data protection law.

reading time: 22 minutes

I. Introduction

By „multiplayer games“ we mean games that can be played by a large number of players simultaneously with or against each other, usually with players from all over the world participating simultaneously and in the same sessions or game worlds. This includes games of different genres, e.g. „Battle Royale“ games (such as „Fortnite“ or „PUBG“), but also online role-playing games¹ such as „World of Warcraft“ or „Elder Scrolls Online“. These games thrive on a certain fairness within the game, which is why their providers take measures to combat unfair play (so-called anti-cheating). This is usually done in a partially automated way and thus raises questions of automated decision making in particular (Art. 22 GDPR). Since the games are basically accessible to a worldwide audience, a transfer of personal data to countries outside the European Union is usually unavoidable in order to be able to offer the service. Therefore, the issue of data transfer in light of the ECJ's Schrems II ruling² is particularly relevant here.

By games on social networks, we mean games that are offered on the major platforms for users registered there, in particular „Facebook Instant Games“ and „Snap Games“.³ Generally, players registered on the social network do not have to create their own user account (account) with the game provider but can use the account of the social network. Many of these games have an „Invite Friends“ function, which makes it very easy to have joint game sessions, especially with existing friends on the respective platform. From a data protection perspective, the tight interlocking with the social networks is particularly important. The first games on social networks were so-called „social games“, most of which also fell under the definition of multiplayer games (see above) (e.g. „FarmVille“)⁴; however, this is by no means the case for all games accessible on social media. Especially the currently popular Facebook Instant Games are usually not multiplayer games. Rather, they thrive on sharing gaming experiences and successes with friends on the social network.

II. Multiplayer Games

1. Anti-cheat

In the vast majority of multiplayer games, the appeal lies (also) in competing with other players. Some of these games rely primarily on direct competition (e.g., Battle Royale games or shooters). But even where competition is less prominent than togetherness, fairness plays an important role: Valuable items, for instance, have to be earned, not „cheated“. For this reason, many providers take action against unfair play.⁵ At the heart of this is the detection of third-party software that gives users advantages not intended in the game or automates game functions (so-called cheats, cheat bots or hacks – hereinafter: cheat software). The providers of this software often act under the protection of anonymity. Such software has been considered a violation of copyright and competition law in numerous court decisions,⁶ but this is not the topic of this article. This article is only interested in the aspects of data protection law. Most multiplayer games use different systems to detect cheat software. Some of these are proprietary systems of the respective game provider, some are third-party software solutions (such as BattlEye⁷ or Easy Anti Cheat⁸), and often a combination of these (hereinafter: anti-cheat technology). These solutions have in common that they analyze various data related to the player in order to be able to detect whether cheat software is being used. Since cheating players are usually permanently excluded („banned“) by the game provider, anonymized processing is usually out of the question.

a) Legal basis

Accordingly, the question of the legal basis arises first. Consent would be conceivable in principle (Art. 6 (1) lit. a) GDPR), but is

not suitable because it can be revoked at any time. Some game providers argue that the use of anti-cheat technology is necessary for the fulfillment of a contract (Art. 6 (1) lit. b) GDPR). We find the recourse to legitimate interests (Art. 6 (1) lit. f) GDPR) more convincing. Of course, in the context of necessity or when weighing up interests, it must also be taken into account how the personal data processed by anti-cheat technology is protected, including within the company. Special attention should thus be paid to technical and organizational measures and short deletion periods.

b) Automated decision-making

In successful multiplayer games, the number of cheating attempts detected each day is considerable. In some cases, the players caught are initially only warned, but as a rule they are directly banned from the game. In the case of large titles, the number of players per day is often in the thousands, according to reports. In the case of the game „Call of Duty: Warzone“ alone, for instance, more than 30,000 players were banned for cheating on one single day, according to the developer.⁹

The decision is at least prepared by the anti-cheat technology. So as not to fall under the fundamental prohibition of automated decision-making under Art. 22 GDPR and not even to have to disclose the logic of the anti-cheat technology under Art. 15 (1) lit. h) GDPR (which would significantly reduce its effectiveness), game providers should at least not make the decision on a definitive ban of a player and the deletion of the corresponding account exclusively by automated means (cf. Recital 71). However, an exclusively automated decision is generally also assumed if a person – without engaging in own considerations – merely confirms or adopts the automated specification.¹⁰

This means that the decision prepared by the anti-cheat technology must be controlled by at least one person. This presupposes that the person has both, access to the necessary data basis and the professional qualification. In addition, the person must have a certain degree of freedom to make decisions, i.e., the person must be authorized to deviate from the automatically prepared decision, if necessary. It is not required that the person performing the review knows the details of the anti-cheat technology or its algorithm.¹¹

As a rule, players who, in the opinion of the game provider, have cheated are initially temporarily banned from participating in the game, i.e. they can no longer participate, but their account

¹ In English abbreviated as MMORPG, for Massively Multiplayer Online Role Playing Game.

² ECJ MMR 2020, 597 with comments by Hoeren = ZD 2020, 511 with comments by Moos/Rothkegel – Schrems II.

³ The importance of MySpace and StudiVZ, both of which also offer social games, has declined significantly in recent years, so these networks will not be discussed in depth below.

⁴ Cf. also <https://www.businessinsider.de/gruenderszene/lexikon/begriffe/social-games/>.

⁵ For a brief legal overview in English, see e.g. Lober, Cheat software: Can publishers level the playing field?, available at: <https://www.gamesindustry.biz/articles/2020-02-05-cheat-software-in-online-games-how-can-publishers-level-the-playing-field>.

⁶ See e.g. BGH judgment of 6 October 2016 – I ZR 25/15 and BGH MMR 2017, 394; see also Conraths, CR 2016, 705 et seq.; Rauda, MMR supplement 8/2019, 20 et seq.

⁷ Cf. www.battleye.com.

⁸ Cf. easy.ac.

⁹ Available at: <https://www.eurogamer.net/articles/2021-05-16-500-000-cheater-s-have-been-banned-from-call-of-duty-warzone>.

¹⁰ Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1st ed. 2019, Art. 22 GDPR, marginal 26 et seq. with references

¹¹ Scholz (Footnote 10 above), marginal 27; Gola/Schulz, DS-GVO, Art. 22 marginal 16; von Lewinski, in: BeckOK DatenschutzR, 36th ed., as of: 1 May 2021, DS-GVO Art. 22 marginal 24.

remains in existence. If the suspicion is not substantiated, they can be reactivated for participation in the game. It is true that this will not be a measure with legal effect but a purely factual restriction. In the area of private law, it is primarily declarations of intent in legal transactions that have a legal effect.¹² Also, there will generally be no significant impairment, provided that the game provider reviews the process in response to a complaint from the player within a reasonable period of time. Hence, according to this view, a temporary blocking of an account could regularly also be performed fully automatically, without a case of Art. 22 GDPR being given. However, in special cases – e.g., tournaments with high prize money – an automated decision proposal should be reviewed again by a person.

No later than before the termination of the game licence agreement and irreversible deletion of an account, the player concerned should have the opportunity to ask for a review of the process carried out by a person, which also corresponds to the guiding principle of Art. 22 (3) GDPR. The termination of the game licence agreement will be a measure with legal effect, the irreversible deletion of an account will at least in some cases be a significant impairment of the player; especially if the player loses significant game progress or „virtual possessions“ as a result.

c) Right to information

It is not uncommon for „banned“ players to assert a claim for information pursuant to Art. 15 (1) GDPR. In this case, the game provider is obligated to provide information about whether personal data of the player is being processed and, if so, to what extent. For this purpose, the law provides for a whole catalog of information to be provided, which includes, among other things, the processing purposes, the categories of data processed, the recipients of data, the storage period and more detailed information about the rights of the data subject (cf. Art. 15 (1) GDPR). Particularly relevant for „banned“ players is the provision set forth in Art. 15 (1) lit. h) GDPR, according to which information must also be provided about the existence of automated decision-making, including profiling, including meaningful information about the logic involved and the scope and intended effects of such processing for the data subject.

Although the right of access is one of the most important rights for data subjects, because it can and should only enable data subjects to identify and exercise their further rights, it is often only needed here for the purpose of finding out the details

about the anti-cheat technology used. So, it is often less a matter of protecting data protection than of knowing the anti-cheat logic involved, e.g. in order to be able to circumvent it in the future or simply to put pressure on the game provider.

In principle, the game provider must fulfill the right of access within the time limit.¹³ Something else only applies in the case of obviously unfounded or excessive requests, which may exist in particular in the case of frequent repetition (cf. Art. 12 (5) Sent. 1 GDPR); nevertheless, the hurdles for this exception are high. However, the lines of the game provider's duty to provide information will have to be drawn where its trade and business secrets are affected. After all, the right to information under Art. 15 GDPR serves to enable the player to review the processing of his personal data by the controller so that he can assert further data subject rights, if necessary (cf. Recital 63 Sent. 1). However, this must not affect the rights and freedoms of other persons, such as trade secrets or intellectual property rights (Recital 63 Sent. 5). It is neither evident nor comprehensible why this restriction should only apply to the benefit of other persons, while the controller who is obliged to provide the information should not be protected with regard to his own protected interests. Consequently, it cannot be the purpose of the right to information to oblige the controller to disclose his own trade secrets. Admittedly, this restriction may also only apply to the extent that the right to information of the data subject does not run dry as a result. However, the interests of the game provider that are worthy of protection, i.e. to protect its game and the guarantee of a fair interaction between the players, must also be taken into account when assessing the scope of the duty to provide information with regard to the disclosure of the anti-cheat technology involved.

2. International data transfer

Multiplayer games are characterized by the fact that they are accessible to participants from all over the world. They play with and against each other. Hence, it is technically almost inconceivable how such services could be realized without a cross-border exchange of personal data. Complete anonymization is also generally out of the question, since at least user IDs must be available that can be assigned to a person by the game provider. Complete encryption of player data transmitted abroad will also not be possible as a rule since it is precisely communication between players in different territories that ought to be possible.

Therefore, in most cases, none of the technical options for data exchange to potentially insecure third countries proposed by the *European Data Protection Board (EDPB)* in response to the Schrems II ruling seems to be a feasible way forward.¹⁴ In particular, the *EDPB* states that in certain situations there are insufficient technical means to protect personal data when cloud services are used and the cloud service provider needs access to unencrypted data.¹⁵ This will also be the case with many multiplayer games.¹⁶

It is also difficult to argue that only a small number of users are affected by such transfers, as generally required by the data protection authorities for the application of Art. 49 GDPR with reference to the requirement of only occasional data transfers.¹⁷

However, this general quantitative restriction is in fact not necessary: If the international data transfer is required, for instance, for the performance of the contract or is based on consent, it may also be carried out en masse. What is necessary, though, is that the consent is informed – also with regard to the specific risks of a data transfer to insecure third countries – or that strict standards are applied to the necessity test when fulfilling the contract.

¹² von Lewinski (see footnote 11 above), BDSG § 6a marginal 25, Scholz (see footnote 10 above), marginal 34.

¹³ The deadline is regularly one month after receipt of the request and may be extended by another two months in exceptional cases if this is necessary taking into account the complexity and the number of requests (cf. Art. 12 (3) GDPR).

¹⁴ Cf. the “Recommendations 01/2020 on measures to complement transfer tools to ensure the level of protection of personal data under Union law” published by the *European Data Protection Board (EDPB)* dated November 10, 2020, available at: [edpb_recommendations_202001_supplementarymeasures_transfer_tools_de.pdf](https://edpb.europa.eu/system/files/2020-06/edpb_recommendations_202001vo.2.0_supplementary_measures_transfer_tools_en.pdf) (europa.eu), new version 2.0 dated June 18, 2021 available at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementary_measures_transfer_tools_en.pdf.

¹⁵ Cf. see footnote 14, marginal 88.

¹⁶ Different, if applicable, if the game servers are all located in the EU or countries with an adequate level of data protection; however, due to latency, game servers are often located in different regions of the world.

¹⁷ Cf. the PR of the Conference of Independent Data Protection Supervisors of the Federation and the German States (*Data Protection Conference*) of 28 July 2020, available at: https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf, which refers to the “Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems” published by the *EDPB* on 23 July 2020 and explicitly confirms the legal opinion there on the narrow applicability of Art. 49 GDPR (No. 8 of the FAQ).

This already ensues from the wording of the GDPR itself, but seems to have been somewhat forgotten: First of all, the heading of Art. 49 GDPR reads „Derogations for specific situations“, thus does not contain any quantitative restriction. Rather, a quantitative restriction is only set out in Art. 49 Sent. 2 GDPR, which reads: „Where a transfer could not be based on a provision of Articles 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data subjects ...“.

This implies that in the cases mentioned in the first subparagraph, no quantitative restriction applies, especially not in the case of informed consent (lit. a) or for the performance of a contract between the controller and the data subject or corresponding pre-contractual measures (lit. b). This is also confirmed for processing based on consent by the recitals; there, however, quantitative restrictions are provided for processing for the performance of a contract (see Recitals 111 and 113). However, the wording of Art. 49 GDPR, which is clear in this respect and does not contain a quantitative restriction even for processing for the performance of a contract, must take precedence over the recitals¹⁸ The recitals serve merely as an aid to interpretation.¹⁹

Incidentally, the strict position of the *EDPB* and the German data protection authorities is all the more surprising because – as far as processing based on consent is concerned – it contradicts the *EDPB* Guidelines 2/2018²⁰, to which explicit reference is made in the *EDPB* Recommendations.²¹

III. Games on Social Networks

1. Responsibilities

The particular feature of games on social networks is that a third party, namely the respective platform operator, comes into contact with the personal data of the players and can process them – depending on the purpose and contractual situation. The fundamental question is of course who is the controller for which data processing operations.

At first glance, it seems obvious that the responsibility for all data processing lies with the platform operator (Facebook, Snapchat or similar). If the user, i.e. the respective player, has agreed to the data protection provisions of the social network when creating his account, this should also apply to all further data processing, i.e. also to the data processing in the game.

Yet it is not quite as simple as that. If data is transferred from the social network to the game provider and processed and evaluated on its own servers, the social network is no longer solely responsible. According to the *ECJ*'s criteria for Facebook fan pages²², joint controllership is in any case obvious. As in the case of Facebook fanpages, there could be a joint determination of purpose and means, and the influence on the data processing is probably to be found here in the design of the game by the publisher. After all, it is up to the publisher to determine which data is collected and processed within the game. However, the classification cannot be made schematically for all games, but must be assessed on a case-by-case basis. The more sparingly the game is designed in terms of data, the less one will assume joint controllership.

The providers of the important social networks currently do not seem to generally assume joint controllership. In any case, no joint controller agreements are provided. Rather, game providers must accept the social network's terms and conditions, which include policies on the use of the gaming platform being docked.²³ These contain different regulations on data protec-

tion responsibility depending on the social network; it is usually assumed that the game provider and the social network are (independent) controllers.²⁴ If the platform provider also takes over the hosting of the games, a data processing agreement is also regularly concluded.²⁵ In this context, standard data protection clauses may also be agreed (for the special features of international data transfer, see III. 3. below).

2. Data processing and legal basis

a) Data from the game

Extensive data processing takes place when playing games on social networks.²⁶ When the user starts a new game session, the social network regularly assigns him an individual identifier (ID) that is linked to the account data. This user ID, together with various other data, is transmitted to the game provider, who needs it to create a player profile for the specific user in the selected game and thus enable him to play on the social network. This data will usually include the (account) name, the language settings, the country in which the user plays, possibly some technical data (such as the operating system of the terminal device), and in the case of Facebook also the profile picture and the „friends“ with whom the user is connected on Facebook and who have also already played the selected game. As soon as the user starts playing, the game duration (running and pausing sessions) as well as the game progress and success (levels reached, high scores, help used, etc.) are recorded for the respective game, and sometimes also the friends with whom the user is playing together. These data are not only processed by the game provider itself in order to provide the game with all its functions. Due to the linking with the user ID assigned by the platform operator, this data is also added to the player profile stored on the platform and thus linked to the player's account on the social network. The platform operator thus receives a lot of data from its users that it would not have without providing the games.

While the platform operator usually obtains comprehensive consent from its users for all data processing on the platform when the account is created, the effectiveness of which will not be discussed further here, the game provider cannot rely on this consent in case of doubt. This consent vis-à-vis the social network, which is often very extensively designed according to the principle of „one size fits all“, cannot in case of doubt also cover the data processing in the game by the specific game provider. It is difficult, for instance, if certain games have not yet been developed and/or offered on the respective platform at the time the account is created. In addition, the user is then already lacking the necessary level of information. Special references to the games are usually not made during the account creation process.

¹⁸ In conclusion also *Schröder*, in: *Kühling/Buchner*, DS-GVO BDSG, 3rd ed. 2020, Art. 49 marginal 11a.

¹⁹ *Simitis/Hornung/Spiecker*, *Datenschutzrecht*, 1st ed. 2019, Introduction marginal 270.

²⁰ Guidelines 2/2018 on exemptions under Art. 49 of Regulation 2016/679.

²¹ Cf. Recommendations 01/2020 (see footnote 14 above), marginal 25.

²² *ECJ* MMR 2018, 591 with comments by *Moos/Rothkegel* = ZD 2018, 357 with comments by *Marosi/Matthé* and with comments by *Schulz* – ULD/WAK Schleswig-Holstein.

²³ For instance, the „Snap Games Platform Terms“, available at: <https://snap.com/de-DE/terms/snap-games-platform>, which are incorporated into the „Snap Developer Terms“, available at: <https://snap.com/de-DE/terms/developer>; for Facebook, the „Developer Guidelines“, available at: <https://developers.facebook.com/devpolicy/>, which are part of Facebook's „Platform Terms of Use“, available at: <https://developers.facebook.com/terms>.

²⁴ Cf. No. 3a of the Snap Games Platform Terms; in the case of Facebook, this results from the data protection obligations that Facebook imposes on game providers, among others in No. 3 and 4 of the Platform Terms of Use.

²⁵ E.g. the Snap Data Processing Agreement, available at: <https://www.snap.com/de-DE/terms/data-processing-agreement>.

²⁶ For more information on data processing in the games industry, see *Bänsch/Hentsch* in this supplement.

As a rule, however, the game provider will not require consent at all, at least not as long as it processes the user data solely for the purpose of providing and implementing the specific game. In this case, the data collection and processing serves exclusively the fulfillment of the contract and is thus justified pursuant to Art. 6 (1) lit. b) GDPR. Of course, the narrow purpose limitation of this data processing on the part of the game provider must be respected.

b) Tracking and analysis

Unsurprisingly, the data generated when playing on social networks is also analyzed. This is done by both the game provider and the platform operator, albeit for different purposes.

The game provider regularly evaluates certain technical data as well as data from the game progress, which is primarily used for error analysis and correction. In this case, the personal reference is usually removed before the evaluation (e.g., by hashing the user ID), because the specific player is not important for the purpose pursued. In addition, the game provider receives aggregated reports and evaluations from the platform operator in order to improve the game offered and to be able to adapt the game to the user needs. These evaluations are based on analyses of the data available (only) to the social networks (such as gender, age and country in which the user is located when playing, number of players, etc.). However, since the game providers do not have access to the platform's account data, they cannot draw any conclusions about individual users.

In view of this, such evaluations can be based on the legitimate interests of the game providers for the purpose of general optimization and improvement of the gaming experience as well as for the elimination of technical errors. In the context of the balancing of interests to be carried out pursuant to Art. 6 (1) lit. f) GDPR, it must not only be taken into account that the specific user regularly remains unidentified for the game provider, but also that the user himself ultimately benefits from the adjustments based on these analyses. Overriding conflicting interests of the user are thus not likely to exist on a regular basis.

c) Displaying of advertising

However, this reaches its limits when user profiles are specifically created in order to use them for other purposes, in particular for personalized advertising. The platform operator analyses and evaluates the data obtained in connection with the games in order to be able to display targeted advertising to the users, especially within the games. The platform operators sometimes expressly reserve this right in the contractual terms and conditions vis-à-vis the game providers,²⁷ while the game providers are pro-

hibited from running their own advertising in the games, and even less so by third-party providers.²⁸

For this type of personalized evaluation of the data, consent is required in favor of the platform operators.²⁹ Whether this is already included in the consent that the user gives when creating his account in the social network may be doubted, but from the point of view of the game providers, this can be ignored.

3. International data transfer

As with multiplayer games, the problem here is that the processing of data often takes place outside the EU, so that the above-mentioned questions related to the *ECJ* ruling „Schrems II“ also arise in this respect. Though the platform providers are regularly based in the EU (usually Ireland), they also have the data processed in the USA by the parent company or on its servers or in international clouds. Consequently, the data protection guidelines of the platform providers usually contain at least a reference to the fact that the standard data protection clauses have been agreed upon between the companies.³⁰ On the one hand, this is almost impossible to control, and on the other hand, it regularly does not bind the game provider, who may, however, be the exporter of personal data. Insofar as the games are hosted outside the EU or the EEA, an agreement on commissioned data processing (DPA) is concluded, in which the standard data protection clauses are also included.³¹ In this respect, however, there are no references to the additional measures now required by the *ECJ* and the *EDPB* to secure a US transfer if this transfer is to be secured by the standard data protection clauses. There is more room for argumentation if the platform providers are more candid and the game provider can enter into dialog with them in this respect in order to verify the existence of suitable guarantees.³²

There are good reasons why the above arguments also apply here. Above all, it must also be taken into account that players who are members of one of the global social networks and consciously decide to play Facebook Instant Games or Snap Games, for instance, regularly accept the risks associated with the international transfer of data. This is also an expression of the informational self-determination of the respective player.³³

IV. Summary

Multiplayer games are usually global, which is why personal data are also transferred to third countries without an adequate level of data protection. This is possible on the basis of appropriately informed consent or as far as necessary for the fulfillment of the contract, even if it happens en masse. The same applies to international data transfers when playing games on the large, globally active social networks. It is an expression of the player's informational self-determination if he registers with such a network and plays there, in particular in order to be able to use the advantages of this social network when playing.

The detection of cheating software in multiplayer players – so-called cheats – requires the processing of personal data on a considerable scale. This can be based on the need to fulfill a contract or – preferably – on legitimate interests. Attention must be paid to suitable and appropriate technical and organizational measures – also within the company. Players convicted of fraud will be banned from the game. In the case of popular games, a large number of players are affected. The decision is at least prepared by anti-cheat technology. The decision to terminate the game licence agreement and delete the account should be made by a human being who has leeway in making decisions. The person does not need to know the details of the anti-cheat technology and its logic.

When playing games on social networks, extensive data processing takes place, including the necessary exchange of data

²⁷ No. 2e. of the Snap Games Platform Terms; in the case of Facebook, this ensues from the overall context of the specifications in the platform terms of use and developer guidelines, in particular taking into account the privacy policy vis-à-vis users, in which the use of data for advertising purposes is explained in detail, available at: <https://www.facebook.com/about/privacy>.

²⁸ No. 2e (last sentence) of the Snap Games Platform Terms; Clause 7: Para. 4b. of the Facebook Developer Guidelines; on Facebook, only the integration of the Facebook Audience Network is permitted.

²⁹ In detail *Baumgartner/Hansch*, ZD 2020, 435.

³⁰ For instance, in the data protection information for companies on the subject of data transfer, available at: <https://de-de.facebook.com/business/gdpr>.

³¹ Cf. the Snap DPA, No. 6 "Data Transfers", available at: <https://www.snap.com/de-DE/terms/data-processing-agreement>.

³² For instance, *Snap Group Limited* points out in its DPA that a transfer of personal data of data subjects from the EU or UK is only carried out if the requirements of Art. 44 to 47 GDPR are met or one of the exceptions in Art. 49 GDPR applies.

³³ Cf. on eCommerce: *Gabel*, in: *Taeger/Gabel*, DSGVO BDSG, 3rd ed. 2019, Art. 49 marginal 7-9; *Lange/Filip*, in: *BeckOK DatenschutzR* (see footnote 11 above), Art. 49, marginal 13-19; *Schröder*, in: *Kühling/Buchner* (see footnote 18 above), Art. 49 marginal 19a.

between the game provider and the platform operator. Insofar as this is done to provide the games, both the data transfer and the data processing by the game provider can be based on contract performance. Evaluations to a certain extent that do not analyze and monetize personal player behavior, but only take place in aggregated form, are regularly necessary to protect the legitimate interests of the game providers. The displaying of personalized advertising by the platform operators, on the other hand, requires consent.

The game provider and the platform operator are each responsible for their own area of data processing. Joint controllership may be considered if these areas are closely interrelated. The more data-saving the game is designed from the outset and the less data the game provider receives about the specific users from the social network, the less joint controllership can be assumed.

For a quick read ...

- Both multiplayer games and games on social networks are mostly global, so personal data can also be transferred to so-called third countries. This may be permissible on the basis of Art. 49 (1) lit. a) or b) GDPR (consent or performance of contract).

- When using anti-cheat technology, attention must be paid to the specifics of automated decision-making pursuant to Art. 22 GDPR. This also applies if claims for information are asserted by players.
- The usual data processing in the context of these games can as a rule be based on the fulfillment of a contract or legitimate interests. Consent in favor of the game providers is in general not required.
- Not only the game providers, but also the respective platform operators are responsible for their own data processing in the social network. Joint controllership can be considered, but does not have to be imperative.



Dr. Andreas Lober
is a partner at Beiten Burkhardt Rechtsanwaltsgesellschaft in Frankfurt/M. and co-head of the practice group IP/IT/Media.



Susanne Klein, LL.M.,
is a partner at BEITEN BURKHARDT Rechtsanwaltsgesellschaft in Frankfurt/M. and a specialist in information technology law as well as a certified data protection officer.

AXEL VON WALTER

User Data, AI, and Automated Decision-Making in Games

Data Protection Requirements for the Use of Automated decision-making in Video Games

Machine Learning

Artificial Intelligence (AI) is, of course, playing an increasingly important role in video games and their monetization. The industry is driving innovation and has long relied on machine learning and AI to make game worlds more believable and the gaming experience more authentic. This also includes the fact that AI can be used more intelligently to combat irregular

game manipulation (so-called cheats). AI recognizes and decides or recognizes and supports decisions. The paper focuses on the specific privacy law requirements for the use of AI and automated decision-making in the video game environment.

reading time: 24 minutes

I. Artificial Intelligence and Games

It is a commonplace that Artificial Intelligence (AI) plays a vital role for modern video games – this also in various dimensions of the product and in relation to the user. After a brief ramble through the main applications of AI in video games, this paper aims to focus on the privacy requirements (in particular, Art. 22 GDPR) for automated decision-making in video games.

1. AI and Gameplay

First, there is the influence of AI on the gameplay itself. Most virtual realities and game settings in modern video games are inhabited by both human-controlled and non-player characters (NPCs). NPCs are increasingly used as AI-controlled virtual agents, neutral characters, hostile opponents, or friendly teammates. The quality of NPCs significantly affects the gameplay and the user's game experience. The requirements for the corresponding AI system are high since the key to the users' game experience is not the NPCs' own goal achievement but the fun of the interaction between users and NPCs. The game

decisions of the NPCs themselves are based on automated decision-making.

To continuously improve the AI-based behavior of NPCs, publishers also rely on machine learning based on users' gameplay and communication behavior. Systematically collecting and evaluating behavioral information can continuously improve the self-learning algorithm for NPC decisions in the gameplay. The collection of user-related behavioral information is used for machine learning, i.e. improving AI. This is to be distinguished from the application of AI e.g. for automated decision-making.

2. AI and Game Testing

Another field for the use of AI in the context of video games is game testing. The more complex the game worlds and interactions between users, other players and NPCs in video games are designed, the more challenging game testing in quality assurance becomes. The complexity of automated testing in this case goes far beyond mere software testing. Compared to general software development, several additional aspects have to be

taken into account in the quality assurance of video games, such as testing the fun factor, testing the game balance, testing the individual game levels/worlds, etc. The AI-based game testing itself is an internal process in the further development of video games and usually has no real user reference in terms of processing of user-related data.¹

3. AI and Anti-Fraud / Anti-Cheat

In practice, the most significant application of AI in the relationship between the publisher and the users of the game are the prevention of fraud as well as anti-cheat procedures. In this context, self-learning automated fraud detection procedures are used both in the gameplay itself and in payment processing. Fraud detection in payment processing serves to ensure the integrity of payment for the use of the game or for in-game purchases of digital goods, or to comply with other regulatory requirements in payment transactions. Fraud detection in the case of video game-based business models does not differ significantly from that of other telemedia providers or in e-commerce.

In addition to payment-related detection methods, AI-based methods for detecting manipulations and unfair influences on the gameplay – so-called cheats – are used primarily for the integrity of the game. Protecting the gameplay from cheats is of vital interest to the game, the users, and therefore the publisher. The publisher thrives on the users' trust in the authentic and uninfluenced gaming experience. Making a long story short: If this trust is only shaken by the suspicion of relevant manipulation by third parties, users will turn away from the game and the business concept of the game publisher, whose budget for the development of a game is often larger than the budget of a big Hollywood film production, will not pay off.

Few details are publicly available on the methods and detection procedures used in anti-cheat measures. Comprehensible secrecy interests of the publishers ensure that many methods in detail have not yet and will never become public. In addition, detection techniques are constantly evolving. Publishers are developing new methods to detect cheaters, while old methods are becoming ineffective and redundant. In general, two categories of detection methods can be distinguished. While client-based methods rather aim at the technical detection and prevention of unfair game influence on the personal hardware of the player (client), server-based methods go for the evaluation of the personal (game) behavior, which can be logged and evaluated on the server side.² Both methods can provide relevant personal data

that can be the basis for the use of AI and automated decision-making.

4. Subfield of AI: Automated Decision-Making

As diverse as the application areas of artificial intelligence are, automated decision-making processes in particular are of great relevance to publishers in practice. Exclusively automated decision-making is the ability to make decisions without the direct involvement of an individual using technical means.³ Automated decision-making processes are also called ADM processes.⁴ In the context of the basic features that characterize „intelligent“ applications – perceiving, understanding, acting, and learning – automated decision-making is a subfield of the „acting“ feature. ADM systems make a decision based on the previous algorithmically mapped knowledge as a machine action and assume the other elements as information acquisition and processing. The benefits for using AI for automated decision-making are obvious. ADM systems can take into account a disproportionately larger amount of information and, ideally, make a neutral and purely information-based decision. So, in practical application, ADM systems give rise to quick, inexpensive, and perhaps better decisions. But ADM systems also have weaknesses, and the decisions made by machines can have noticeable consequences for people.

In practice, the decision-making process of ADM systems is usually not very transparent. First, because decisions are made in a systemic black box.⁵ Second, because the underlying algorithms remain well-guarded as trade secrets of the developing companies. Inadequate data can lead to covert discrimination and have far-reaching consequences for people's lives. There are individual specific legal regulations for the general prevention of discrimination. However, the GDPR in particular fundamentally aims to protect people from becoming the object of fully automated decision-making by machines in their life and social sphere.⁶ In the following, this paper will take a closer look at the data protection perspective on the use of ADM systems in the area of video games.

II. Automated Individual Decision-Making, Including Profiling

The basic regulation for the question of the admissibility of ADM systems is found in Article 22 (1) GDPR.⁷ It states that everyone has the right „not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.“

Paragraph 2 exempts automated decisions necessary for the conclusion or performance of a contract between the data subject and the controller (lit. a) and automated decisions with the data subject's explicit consent (lit. c) from the prohibition in Paragraph 1. Paragraph 4 contains a carve-out for special categories of personal data pursuant to Article 9 (1) GDPR.

In general, Article 22 (1) GDPR prohibits a fully automated decision in an individual case which has legal effect or similarly significantly affects (principle). However, there are exceptions from this principle: If and to the extent that an exception to the principle applies, measures must be implemented to safeguard the rights and freedoms as well as the legitimate interests of the data subject, including information about the processing as well as the possibility of human intervention in the decision-making process.⁸

The data processing necessary for automated decision-making can only be justified via the permissive elements of Article 6 and Article 9 GDPR. Article 22 (1) GDPR is not a legitimizing legal ba-

¹ Therefore, game testing will only be mentioned here as another example of an application area of AI for video games but will no longer play a major role for the further discussion of the data protection aspects of automated decision-making.

² Issues related to client-based data analysis and the Directive 2002/58/EC (Directive on privacy and electronic communications) can be left out for this paper, as this is about automated decision-making based on the collected data.

³ Cf. definition in wp251rev.01 „Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679“, p. 8.

⁴ „ADM“ stands for Algorithmic decision-making.

⁵ ADM systems make decisions in systems that consist of several layers of artificial „neurons“ and each layer uses self-learning algorithms so that an operation that passes through several layers is hardly comprehensible to humans and that is why AI systems are also referred to as „black boxes“; see *Stiemerling*, in: Kaulartz/Braegelmann, *Rechtshandbuch Artificial Intelligence und Machine Learning*, ch. 2.1, marginal no 6 et seqq. on the technical background of AI and the systems.

⁶ Cf. Recital 71 p. 1 GDPR.

⁷ Article 9 (1) lit. a of Council of Europe Convention 108, as revised following the adoption of the 2018 Protocol, also contains a prohibition on subjecting individuals to a decision if the decision is solely automated. However, the prohibition only applies if the decision has a significant impact on the data subject.

⁸ Cf. Recital 71 p. 4: „In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.“

sis for automated decision-making, but rather a supplementary restriction for the fully automated processing of personal data in the event that the processing produces legal effects vis-à-vis the data subject or significantly affects him or her in a comparable manner.

Article 22 GDPR is not a restriction on AI itself. Rather, the regulation is merely a restriction on the use of artificial intelligence.

Decisive for the question to what extent automated decisions can be used in the environment of video games within the scope of the GDPR is whether it is a completely automated decision with a relevant effect for the data subject or whether there is a legal exception to the general prohibition.

1. Automated Decision

Since the prohibition of Article 22 GDPR aims to protect data subjects from becoming the object of machine decisions, it only applies in cases in which machine – i.e. automated – decisions are made without any human decision-making influence. In other words, there is no room for the prohibition of data processing if either no decision is made or the human being is ultimately involved in the data processing.

a) Decision or Mere Execution?

The prohibition in Article 22 (1) GDPR only applies to „decisions“. The term „decision“ is not defined in the GDPR. A decision does not exist if „if-then“ rules agreed in advance between the data subject and the controller are processed by machine. The automated execution of previously mutually agreed consequences is not a decision because there is ultimately no autonomous evaluation, consideration, or exercise of discretion.⁹

If the publisher only mechanically implements if-then mechanisms contractually agreed upon with the user within the game-play or anti-cheat measures, this automated data processing does not constitute a decision within the meaning of Article 22 (1) GDPR. This refers to binary decision structures that are processed by machines. If, for example, the publisher includes rules in its terms of use that follow a binary violation/sanction principle, the mere automated execution of these predefined rules cannot constitute an automated „decision“. However, insofar as AI-based assessments play a role within the data processing, which in the human decision-making process would be referred to as the exercise of discretion, this is a decision within the meaning of Article 22 GDPR, in accordance with the protective purpose of the provision.

b) The Missing Human Factor

Only decisions that are exclusively based on automated processing are subject to the prohibition in Article 22 (1) GDPR. Only then is there no influencing involvement of a human being and the decision is made purely by machine. In order to ensure the involvement of a human being in the decision, according to the prevailing view, the involvement of the human being in the decision must not be a mere fudge. There must be sufficient room for human judgment and final decision.¹⁰ Ultimately, the human being must include other aspects in his decision. After all, even a human decision that simply implements the machine „decision proposal“ is ultimately also based exclusively on machine processing. Even if the automated processing and the decision-making action do not coincide, an automated decision within the meaning of Article 22 (1) GDPR may still exist. The situation is different in the case of mere decision support or decision preparation by intelligent systems. Article 22 GDPR does not aim to prevent decision support and preparation by automated processes.¹¹ If AI supports humans in their decision-making, this does not constitute an exclusively automated decision. If the AI

supports the human being by making the decision with significant legal or other effects for him, this application is subject to the fundamental prohibition of Article 22 (1) GDPR. The distinction is often a question of the individual case, which, however, has a high practical relevance especially in connection with cheat detection. This is because publishers rely on automated detection systems, especially in the area of cheat defense, which can lead to consequences for the player if there is a well-founded suspicion of cheating – from time bans to termination of the contractual relationship. Here, systems prepare or make decisions.

Insofar as the publisher's anti-cheat team has the right to override the prohibition decision proposed by the automated system, the human factor has a determining character and there is no case of Article 22 (1) GDPR. If the publisher's anti-cheat team has limited influence before imposing a temporary ban, e.g. only has the right to verify that the proposed ban decision is free of obvious errors, this will not qualify as sufficient human involvement.

However, even decisions based on the human influence of a third party are not exclusively mechanical decisions within the meaning of Article 22 (1) GDPR. If, for example, a decision by the system to block a user account or player profile is based solely on user complaints, there is no „automated decision“. The anti-cheat logic here merely technically enforces the decision of humans. In this case, the decision to block is based on an interaction of the publisher's pre-defined criteria with the decision of the masses (e.g. other players who have submitted complaints/blocking proposals). The decision here is ultimately not triggered by a human being, but by a number N of humans; consequently, the user does not become the object of an exclusively machine-based decision.

2. Relevant Impact on the Data Subject

There is agreement that only automated decisions that have a relevant impact on the data subject should be covered by the prohibition in Article 22 (1) GDPR. According to the wording of the regulation, alternatively (a) any „legal effect“ or (b) a „similarly significant“ effect is sufficient.

a) Legal Effect

Only decisions that establish, change, or cancel a legal position shall have legal effects.¹² This may concern the legal status of a person as well as the rights of a person under a contractual relationship.¹³

Ultimately, a real legal effect in the relationship between publisher and user can only be considered in practice at the level of the usage agreement. It does not matter whether the usage relationship is structured in return for payment or free of charge. It is only the legal effect that matters, i.e. the existence or non-existence of claims or legal positions. Thus, if the decision to terminate a contractual relationship is based exclusively on an automated decision, this will have a legal effect and the prohibition of Article 22 (1) GDPR will apply. In practice, however, the termination of the contract is first preceded by a warning or a temporary blocking of the user account. It remains disputed whether the warning – which has its own legal significance in the context of an extraordinary termination of the contract in accordance

⁹ Simitis/Hornung/Spiecker gen. Döhmman/Scholz, GDPR, Article 22 marginal no 17, 18 also makes this clear in the concept of “being subject”.

¹⁰ Cf. also *article 29 working party*, wp251rev.01 dated 6.2.2018, p. 22.

¹¹ Cf. Paal/Pauly/Martini, *Datenschutzgrundverordnung*, 2nd edition., Article 22 marginal no 20.

¹² Gola/Schulz, *DS-GVO*, 2nd edition., Article 22, marginal no 22.

¹³ Cf. also *article 29 working party*, wp251rev.01 dated 6.2.2018, p. 23.

with section 626 BGB (German Civil Code) – already has a real legal effect or not. The temporary blocking of a user account could also be regarded as having legal effect, as this constitutes the publisher’s at least temporary refusal to perform under the contractual usage relationship.

b) Similar Significant Effects

Ultimately, however, comparable significant effects are also sufficient for a ban on data processing pursuant to Article 22 (1) GDPR. It is difficult to define which effect on a person is to be considered significant within the meaning of Article 20 (1) GDPR.¹⁴ If the automated decision is likely to affect the circumstances, behavior or decisions of the data subject, affects the data subject over a longer period of time or permanently, or, in the worst case, leads to exclusion or discrimination, the materiality threshold should be exceeded in any case. This is true for decisions that affect financial aspects of a person, decisions about access to health services, decisions about access to jobs, or decisions about access to education.¹⁵

According to another view, it follows from the word „affect“ that in principle only onerous decisions, but not favorable decisions, are to be covered by Article 22 GDPR.¹⁶ If one follows this view, the admissibility of the automated decision ultimately depends on the result of the processing operation: If the automated decision is positive for the data subject, there is no „significant“ effect and the automated decision-making is ultimately in compliance with Article 22 GDPR. If the machine decision is negative, this results in an „effect“ and thus inadmissibility. Correctly, however, one must assume that all automated decisions with a significant effect, regardless of their outcome, fall within the prohibitive scope of Article 22 (1) GDPR. The wording argument from the German version of the GDPR that is based on the word „beeinträchtigt“ (impaired) is significantly weakened by both the English and French language versions of the GDPR. The terms „affect“ or „l’afectant“ can also be understood there as „concern“ or „touch“. Ultimately, the meaning and purpose of the regulation also speak in favor of a neutral understanding and the inclusion of all automated decisions with a significant impact on the data subjects. The aim of the regulation is to protect the human being in its essential aspects determining the circumstances of life, not to become the object of a purely mechanical decision. The essence is that the person must not be „degraded to the mere object of computer operations“ and that responsibility for decisions about people must not be anonymously attributed to computer systems.¹⁷

Therefore, one can ultimately argue whether an automated decision in the context of a video game is at all suitable to exceed the materiality threshold of Article 22 (1) GDPR. Only exceptionally will decisions affect gameplay and participation opportuni-

ties affect the essential circumstances of the user’s life. This may be the case for players in well-paid eSports tournaments. For the casual gamer, it will not be about significant financial issues or access to earning opportunities.

Finally, it is also obvious that the system-based decisions for the gameplay of the NPCs in the game itself do not constitute a „significant effect“ in the legal sense and thus all AI-based game decisions that are inherent to the product and are also expected by the players as a basis for the most authentic gameplay possible are of course not subject to the prohibition of Article 22 (1) GDPR – even if the AI-controlled final boss ultimately defeats the user „by machine learning“.

3. Exceptions from the Prohibition of Automated Decision-Making

There are also legal exceptions to the general prohibition of automated decision-making with a relevant impact on the data subject that may be viable for the use of ADM systems in the context of video games.

a) Establishment and Performance of the Contract

According to Article 22 (2) (a) GDPR, the prohibition of automated decision-making does not apply, for example, if the decision is necessary for the conclusion or performance of a contract between the data subject and the controller. This exception is of great practical relevance if you want to use AI to initiate, conclude and live contracts. The exception is in principle applicable to all contracts between the data subject and the controller. Automated decision-making does not have to be the main subject matter of the agreement but can facilitate or even enable the execution of the contract. Nevertheless, this exception is limited to necessary automated decisions. Because the provisions in Article 22 (2) GDPR are exceptions to the general prohibition in Article 22 (1) GDPR, the criterion of necessity must also be understood narrowly. The controller must consider whether a less privacy-invasive procedure could also be used.¹⁸ Automated decisions may also be required in the performance of contractual relationships, especially when decisions are necessary in fractions of a second. It is questionable, however, whether anti-fraud and anti-cheat procedures can be regarded as necessary for the performance of the contract within the meaning of the exception. For fraud prevention, it becomes more difficult to establish necessity, just as in other business models measures to prevent fraud in the billing of services (credit card fraud) are not seen as a necessary measure for the performance of the contract. For video games and in-game cheat defense, however, the case is different. As the German Federal Supreme Court (*BGH*) has already ruled, competitive equality in multiplayer games is an integral success factor for the game.¹⁹ If equality of opportunity and competition in the game is not ensured, players will turn away from the game, according to the *BGH*. If one follows this statement, it corresponds to the expectation of the players that equal opportunities and competition prevail in the game according to the applicable game and usage conditions. The manipulating player also participates in the game in the expectation that at least the majority of the other players will adhere to the applicable competition rules. Consequently, the anti-cheat procedure can be regarded as data processing necessary for the performance of the contract as a whole and thus as fulfilling the exceptional circumstances of Article 22 (2) (a) GDPR.

b) Consent to ADM

In addition to the statutory exceptions, the data subject may give his or her „explicit“ consent to the processing of data for automated decision-making pursuant to Article 22 (2) (c) GDPR. The

¹⁴ Article 29 working party, wp251rev.01 dated 6.2.2018, p. 23.

¹⁵ Cf. the examples of article 29 working party, wp251rev.01 dated 6.2.2018, p. 24.

¹⁶ Cf. Schulz (footnote 12 above); Taeger/Gabel/Taeger, DSGVO, 3rd edition., Article 22 marginal no 47.

¹⁷ Dammann/Simmitis, Datenschutzrichtlinie, Article 15 marginal no 2; Kühling/Buchner/Buchner, DS-GVO, 2nd edition., Article 22 marginal no 11; cf. also the Resolution of the 97th Conference of the Independent Data Protection Authorities of the Federal Government and the Länder (Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder), 3 April 2019 („Hambacher Erklärung zur Künstlichen Intelligenz“, engl.: Hambach Declaration on Artificial Intelligence), p. 3.

¹⁸ Article 29 Data Protection Working Group, WP 251rev.01 of 02/06/2018, p. 25; EDPS, Assessing the Necessity of Measures Restricting the Fundamental Right to Protection of Personal Data: A Toolkit., 11 April 2017, p. 7.

¹⁹ Federal Supreme Court (*BGH*) MMR 2017, 394, marginal no 70 – World of Warcraft II: „The success of such a game stands or falls on the fact that the same conditions apply to all players for completing tasks and reaching higher levels.“

requirements and conditions for consent from Article 7 GDPR also apply here. Additionally, the statutory exception requires „express consent.“ The consent must therefore be expressly related to one or more specific automated decision-making processes. According to the legal system of Article 22 GDPR, the express consent to automated decision-making pursuant to Article 22 (2) (c) GDPR merely exempts the data subject from the fundamental prohibition of automated decision-making with significant effects for the data subject.

This consent must be distinguished from the consent-based authorization facts of Article 6 and Article 9 GDPR. It is a question of the concrete formulation of the consent whether this consent can have a double legitimizing effect. On the one hand, as legal basis for the data processing as such pursuant to Article 6 (1) (a) GDPR and, on the other hand, as basis for automated decisions within the scope of this data processing. It would also be conceivable to base the data processing on a legal justification in the catalogue of Article 6 and Article 9 GDPR and only allow the form of automated decision-making based on consent. The consent is – like all consents – in principle revocable at any time.

4. No ADM for Data on Ideology, Body and Health

Special categories of personal data (Article 9 GDPR) may not be used for decisions based on automated processing, even if a legal exception of Article 22 (2) GDPR applies. This relates to all personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9 (1) GDPR).

Thus, to the extent that automated and relevant automated decisions are based on bodily data or data on ideology, such data processing operations are subject to the prohibition of Article 22 (1) GDPR and cannot be legitimized via the statutory exceptions of Article 22 (2) GDPR. What at first glance seems far-fetched in the games context is not so at second glance: automated procedures for detecting hate speech, for example, can be based on information about the ideology of the data subject, just as the collection and evaluation of body-related information such as pulse beat or eye movements are conceivable in the field of eSports and competitive gaming in real time.

However, special categories of personal data may also be included in automated decisions if explicit consent to the processing of special categories of data has been given.

5. Appropriate Safeguards for Data Subjects

If the basis for the automated decision is either a contractual relationship (Article 22 (2) (a) GDPR) or consent (Article 20 (2) (c) GDPR), the controller shall take reasonable steps to safeguard the rights and freedoms and legitimate interests of the data subject, in accordance with Article 22 (3) GDPR. This should include, at least, the right to obtain human intervention on the part of the controller, to express one's own point of view and to contest the decision.²⁰ According to Recital 71, the safeguards for processing for automated decision-making must in any case additionally include specific information to the data subject. Transparency in processing and automated decision-making is essential to address the fundamental concerns about automated decision-making.

This also includes measures to prevent errors in decision-making and, in particular, to prevent discrimination. This starts much earlier, because the basis for automated decisions is ultimately the training data as well as the database on which the ADM sys-

tem operates. However, if the selection of training data is poor, the result of processing by AI will also be correspondingly poor. Measures to protect the rights and freedoms and the legitimate interests of the data subjects must already take effect during the training of the system. These preventive measures should also be documented for the data protection impact assessment. In practice, the appropriate protective measures can be implemented in a four-step process:²¹

1. Ensuring that the database is non-discriminatory: Training data as well as the machine e-learning process are carefully and representatively selected and maintained to avoid „biased data“. Data origin and collection context should be documented.²²

2. Information of data subjects: The data subjects shall be generally informed about the fact of the automated decision. This information includes meaningful information about the logic involved and the scope and intended effects of such processing (Article 13, Article 14 GDPR) and the rights under Article 20 (3) GDPR.²³ In this context, „Explainable AI“ should preferably be used.

3. Information on reasons for refusal: In the event of an automated decision unfavorable to the data subject, the reasons for the refusal shall be communicated and explained to the data subject upon request, as provided for in Recital 71. Only with this information is the data subject able to exercise his or her further rights under Article 22 (3) GDPR.

4. Review and correction of the decision: The data subject has the right to remonstrance of the machine-based decision and an intervention of a person on the part of the controller. The affected data subject's own point of view must be heard and, if necessary, the machine-based decision corrected. To this end, the data subjects must be provided with the simplest possible procedures and communication access to the controller.

III. Summary

Artificial Intelligence already has its place in the videogame ecosystem and will continue to grow in importance for the industry. Not all areas of application of AI are relevant under data protection law, but the requirements of the GDPR are particularly relevant for automated decision-making. At first glance, anti-fraud and anti-cheat procedures based on automated systems seem like prime examples of the fundamental prohibition of exclusively machine-based decisions about relevant interests of the users concerned.

On closer inspection, however, there is much to suggest that these measures are not in irresolvable conflict with Article 22 GDPR. In many cases there will be no automated decision, because either the real decision is already missing or it is essentially determined from the beginning by one or more human beings. Further, it is doubtful that all anti-cheat rulings have any notable impact at all on the data subjects involved. Not every minor decision should be prohibited by the dignity-protecting Article 22 GDPR. Finally, an effective anti-cheat system – even if it contains all of the prohibitive features of Article 22 (1) GDPR – may constitute data processing necessary for the performance of the contract. In each case, the publisher will provide appropriate safeguards for the use of AI to make or prepare decisions.

²⁰ Cf. also Recital 71, p. 5.

²¹ Based on Schulz (footnote 12 above), marginal no 42.

²² Cf. in this respect *Article 29 Data Protection Working Group*, wp251rev.01 dated 02/06/2018, p. 31 as well as proposals for measures p. 36 et seq.

²³ Cf. also see footnote 19.

For a quick read ...

- For automated decision-making in and around video games, the requirements of the GDPR are relevant.
- If the AI makes entirely automated decisions that are of significant relevance to the natural person concerned, the GDPR only permits this within very narrow limits and exceptions.
- At first glance, anti-cheat procedures based on automated systems seem like prime examples for prohibited automated decisions.

- When analyzing the decision, in most cases there will be no exclusively machine-based decision or the decision is contractually required.
- In any event, the publisher will provide appropriate safeguards for the use of AI to make or prepare decisions.



Dr. Axel von Walter

is partner at the law firm GvW Graf von Westphalen, certified specialist in copyright and media law, certified specialist in IT law and lecturer in media and information law at the faculty of law at the Ludwig-Maximilians University of Munich.

FLEMMING MOOS

GDPR Enforcement by means of fines using the example of the games industry

What can gaming companies learn from previous fine notices?

Sanctions

This article analyses the practice of enforcing the GDPR by means of fines in the first three years after its entry into force. A special focus is placed on the games industry. In addition to a description of enforcement practice, the article also high-

lights and discusses the legal problem areas that arise when imposing fines on companies for violations of the GDPR.

reading time: 25 minutes

I. Introduction

A good three years after the General Data Protection Regulation (GDPR) came into force, a first conclusion can be drawn as to whether and how consequently the stricter data protection rules are actually applied and, above all, enforced in practice. Many companies, and in some cases entire industries, were in a state of panic before May 2018, with fears of fines in the millions destroying their very existence doing the rounds. The games industry was also gripped by the GDPR panic.¹ In addition, reports were made that some games providers, primarily of US provenance, had withdrawn from the European market because they could not (economically) meet the GDPR requirements or because the risk of sanctions was incalculable. With the possibility of imposing fines of up to 20 million euros or in the case of businesses even up to 4% of the worldwide annual turnover, the data protection authorities certainly have a very sharp sword.

And indeed, it can be stated that in the meantime – often accompanied by extensive press coverage² – a considerable number of fines in quite substantial amounts have been imposed by European data protection supervisory authorities. Everyone is aware of the millions in fines imposed on internet companies,

fashion and real estate companies and telecommunications service providers.³ Just as we are finalising this article, it has been reported that the *Luxembourg data protection supervisory authority* intends to fine *Amazon* 350 million euros⁴ – it would be by far the highest fine for a data protection breach to date. But are these figures a useful yardstick for other companies – especially those in the games industry?

1. Overview of the practice of fines

In general, the amount of the fine alone can only provide a limited indication of the severity of the sanction, because it is influenced by various assessment criteria and – to a significant extent – also by the turnover of the company concerned. Even an amount that appears rather small in the abstract can therefore represent a severe sanction, e.g. because the company only generated low turnover or because the sanctioned violation was marginal. Conversely, a fine in the millions for a company with a turnover in the billions may nevertheless represent a comparatively mild sanction. In this respect, general deductions from these individual case decisions are generally difficult.

In addition, the approach of the supervisory authorities in the various EU member states differs considerably: there are several member states in which there is indeed a lively enforcement practice, but the fines have so far been very moderate (e.g. Hungary with a maximum fine of 288,000 euros, Belgium with 600,000 euros or the Netherlands with 900,000 euros). In addition to the level of sanctions, the density of controls is also relevant for the assessment of the risk of sanctions. Here, too, there is a high disparity between the individual Member States: a particularly large number of fines have been imposed so far in Spain and Germany (with over 200 each), Italy, Romania and Hungary. In contrast, the Member States Ireland, Croatia, Portugal and –

¹ Characteristic of this is, for example, the article in W&V in May 2018: Does the GDPR threaten video games like League of Legends?; available at: https://www.wu.v.de/tech/bedroht_die_dsgvo_videogames_wie_league_of_legends.

² S. on this: *Schefzig/Rothkegel/Cornelius*, in: *Moos/Schefzig/Arning*, *Praxishandbuch DSGVO*, Kap. 16 Rn. 59 ff.

³ A good overview of the fines imposed by European supervisory authorities is provided by the "GDPR Enforcement Tracker", available at: www.enforcementtracker.com.

⁴ Cf. the report on [heise.de](https://www.heise.de/news/Datenschutz-Luxemburg-plant-350-Millionen-Euro-Strafe-fuer-Ama-zon-6068245.html) dated 11.6.2021, available at: <https://www.heise.de/news/Datenschutz-Luxemburg-plant-350-Millionen-Euro-Strafe-fuer-Ama-zon-6068245.html>.

as long as it still belonged to the EU – Great Britain, have only known very few fines in relation to their size.

2. Games companies as addressees of fines

Nevertheless, if one tries to filter out the hundreds of fines that have been imposed in the EU in the last three years in accordance with the GDPR, the following picture emerges where games companies were specifically affected:

In fact, the only known case was a fine imposed by the *Czech data protection supervisory authority*, in which an amount of no less than 980 euros was imposed on a gaming company. What had happened? In an online role-playing game, unauthorised persons were able to access the data of registered players of the platform due to insufficient security precautions.

Initially, the game operator faced a successful DDoS attack by an attacker. The game operator took measures to improve security, yet further hacking attacks were successful. Against payment of a sum of money, the attacker agreed to stop the attacks and help the operator secure the server. The game operator agreed and the attacker provided the operator with a firewall, which the operator installed on his game server after checking it. However, the attacker had secretly built a backdoor into the source code and gained access to the player database. The attacker published the player database and redirected the game's website to his website. The player database contained approximately 4,500 accounts (username, password in encrypted form, email addresses, IP addresses, payment information such as current payment status, number of virtual currency purchased, account holder, time and method of payment) and was published on the internet for approximately 1.5 hours. The operator immediately interrupted the operation of the game and database server, filed a criminal complaint and reported the violation to the persons concerned and the data protection authority.⁵

The *Czech data protection authority* saw this as a violation of Art. 5(1)(f) of the GDPR. In their opinion, the operator should not have had the system „improved“ by the person who was the originator of the DDoS attack. In addition, the DPA found that the game operator used the services of two processors without having concluded processing contracts within the meaning of Art. 28(2) of the GDPR. The *Czech data protection authority* imposed a fine of CZK 25,000 (equivalent to approximately EUR 980).

No further GDPR fines against games companies have become known to date. At most, the fine against a Spanish gaming arcade chain may be worth mentioning, which had installed a video surveillance system in violation of the GDPR, which also covered the public street. The *Spanish data protection supervisory authority* assessed this as a violation of the principle of data minimisation from Article 5 (1) (c) of the GDPR and intended to impose a fine of 6,000 euros, which was reduced to 3,600 euros against immediate payment and waiver of appeal.⁶

3. Processing circumstances at games companies with sanction potential

But does this mean that games companies can sit back and relax because they are supposedly not in the focus of the supervisory authorities? That would certainly be a fallacy as well.

On the one hand, industry affiliation is not really a relevant criterion in itself. It is true that data protection supervisory authorities do structure their proactive monitoring activities in such a way that they carry out audits specifically in certain sectors. However, this is the exception rather than the rule. On the other hand, it should be noted that the data processing of games companies⁷ does have some characteristics that make them „danger-prone“

processing; for example, the often large volume of player data processed, the extensive online tracking possibilities or sometimes the youth of the players to whom the data refers.

A relevant risk factor is also the issue of data security. Especially online or platform games are in the focus here. Often, the consequences are not as benign as in the above-mentioned case of the Czech game provider: According to media reports, the hacker, known in the scene under the pseudonym *Gnosticplayers*, recently captured a total of approximately 200 million user data from a US game provider.⁸

Especially in the latter cases of a data breach, there is often a supervisory „aftermath“. In the course of further investigations of data breaches reported to them under Article 33 of the GDPR, it is standard procedure for data protection supervisory authorities to check whether their own failures in data security may have been partly responsible for the loss of the data. If this is the case, there is indeed the threat of fines. This has been particularly prominent in the *Marriott*⁹ and *British Airways*¹⁰ cases, but a focus on sanctions in the area of data security due to a lack of technical or organisational measures is also evident among German supervisory authorities:¹¹

■ After the hacker group *Magcart* succeeded in stealing the personal data and payment information of 500,000 customers within two weeks with the help of skimming scripts, the British data protection authority *ICO* imposed a fine on *British Airways* for inadequate security measures because these had made the hacker attack possible in the first place.

■ In the *Marriott* case, hackers had compromised the payment information and personal data of 500 million customers of the hotel chain. Although the infiltration of the company's network took place four years ago and at a time when the subsidiary in question was not yet part of the *Marriott group of companies*, the *ICO* found that *Marriott* had culpably failed to carry out the necessary checks as part of a data protection due diligence when it bought the company.

As an interim conclusion, the games industry has so far – as far as the public knows – been largely spared from the enforcement of the GDPR in monetary terms by means of fines. Unfortunately, this is not an all-too-comfortable resting place: the data processing of many games companies is definitely risky in several respects, so it should only be a matter of time before we also see increased enforcement by means of fines in the event of violations.

II. Current problem areas in the sanctioning of companies by means of fines under the GDPR

However, even if a games company is found to be in breach of the GDPR and the competent authority wants to sanction it with

⁵ For details see <https://www.uoou.cz/kontrola-zabezpeceni-osobnich-udaju-pri-provozovani-online-hry-fyzicka-osoba-podnikajici/ds-5723/archiv=0&p1=5653>.

⁶ Decision of the *AEPD* v. 15.4.2019, available at: <https://www.aepd.es/es/documento/ps-00135-2019.pdf>.

⁷ See the article by *Bänsch/Hentsch* in this supplement.

⁸ Cf. the report on *golem.de* as of 1.10.2019, available at: <https://www.golem.de/news/mobile-games-datenleck-bei-spielehersteller-zynga-1910-144188.html>.

⁹ Cf. the report on *e-recht24.de* dated 3.11.2020, available at: <https://www.e-recht24.de/news/datenschutz/12429-marriott-bussgeld-corona.html>.

¹⁰ Cf. the report on *netzpolitik.org* dated 9 July 2019, available at: <https://netzpolitik.org/2019/dsgvo-british-airways-soll-rekordstrafe-wegen-sicherheitsmaengeln-zahlen/>.

¹¹ Cf. the reports on *lto.de* dated 11.11.2020, available at: <https://www.lto.de/rec ht/nachrichten/n/lg-bonn-29owi120lg-bussgeld-1und1-datenschutzverstoss-dsgv o-millionen-herabgesetzt/> and on *heise.de* dated 22.11.2018, available at: <https://www.heise.de/newsticker/meldung/Passwoerter-im-Klartext-20-000-Euro-Bussgeld-nach-DSGVO-gegen-Knuddels-de-4229798.html>.

a fine, this is by no means the end of the world. It has been shown that it is not at all easy for the supervisory authorities to issue corresponding penalty notices in a legally compliant manner. A few very current stumbling blocks in connection with the imposition of fines, which can be used against the legal conformity of a fine, are therefore pointed out below.

1. Selection of the debtor of the fine

Supervisory authorities sometimes enter legally uncertain territory when selecting the party liable to pay a fine. By law, a fine pursuant to Article 83 (4), (5) and (6) of the GDPR is imposed on the controller of the respective data processing, whereby processors can also be directly fined.

a) Imposition of a fine in the case of multiple participants

If more than one party is involved, sanctions must be imposed separately depending on the share of fault,¹² Section 41 (1) sentence 1 BDSG in conjunction with Section 14 (1) OWiG. Section 14 (1) sentence 1 OWiG stipulates that if several persons are involved (e.g. two jointly responsible persons), they are both guilty of an offence (and can therefore each be the addressee of a separate penalty notice).¹³ In contrast to Article 82 (4) of the GDPR, Article 83 of the GDPR does not provide for joint and several liability of several controllers or controllers and processors working together.

b) Imposing fines on affiliated companies

In practice, however, supervisory authorities sometimes impose fines on companies that are not even accused of a data protection violation. Cases have come to light in which a fine was (also) imposed on the parent company of the responsible party. As justification, the supervisory authorities refer to the so-called anti-trust law concept of an undertaking,¹⁴ which shall also be applied here in the context of the GDPR.¹⁵ According to this definition, an undertaking is any entity carrying out an economic ac-

tivity, regardless of its legal form and the way it is financed.¹⁶ The decisive argument for a corresponding connection in data protection law is the reference in recital 150, sentence 3 of the GDPR to Articles 101 and 102 TFEU. The effect of this is that the definition of „undertaking“ in Art. 83 GDPR does not refer to the legal subject, but functionally to the economic entity.

This initial thesis is already extremely controversial and there are very good counter-arguments. For example, it is significantly countered that Recital 150 should not overwrite the actual norms of the GDPR, which is why the definition of Art. 4 No. 18 GDPR should be used and thus a company should not be equated with a group of companies (Art. 4 No. 19 GDPR).¹⁷ This line of argument is supported by the established case law of the *CJEU*, according to which contradictions between the wording of recitals and the actual legal text are to be resolved in favour of the latter.¹⁸

However, it also seems questionable to designate a company as the subject of liability solely on the basis of the existence of a connection under company law with the offender. The wording of Article 83 (2) and (3) of the GDPR stipulates that only controllers and processors can commit infringements subject to fines – and consequently only they can be the addressee of a fine.¹⁹ Nothing else follows from Article 83 (4), (5) and (6) of the GDPR and Recital 150, because these provisions only regulate the amount of the fine, but do not extend the group of possible addressees of the fine.²⁰ Any other interpretation seems incompatible with the principle of „nulla poena sine lege“.²¹

A parallel to competition law is not possible because the legal situation under the GDPR is different: In contrast to the prohibition of cartels, the GDPR rules are not directed at „undertakings“ in the abstract, but at controllers and processors. Therefore, in contrast to competition law, data protection law is not based on the principle of the functional entity, but on the principle of the legal entity.²² However, because there is correctly no separation between the violation (factual side) and the substantive liability addressee (legal consequence side), the liability for fines can only be imposed on the legal entity that also committed the violation.²³ The inclusion of e.g. the parent company of the infringing enterprise in the penalty notice is therefore only possible if it is liable for a fine under data protection law – for example as a processor or as a jointly responsible party. However, the mere fact of being an affiliated company does not justify the issuance of a penalty notice against the parent company.²⁴

2. Conditions for imposing a fine on a company

No less shaky is often the reason given by the supervisory authority for imposing a fine on a company – i.e. as a rule a legal entity – at all. This is by no means as self-evident as it may seem in view of the large number of fines now imposed under the GDPR.

German law (beyond competition law) is fundamentally unfamiliar with the approach enshrined in the GDPR that a legal person can itself be the addressee of a fine as an undertaking within the meaning of Art. 83 GDPR. In German law, there are therefore the attribution norms in the OWiG, in particular Section 30 OWiG, which contain the necessary requirements for a legal person to be fined.

The authorities have so far taken the position that Art. 83 of the GDPR imposes direct liability on the company and that the provisions of Sections 30 and 130 of the OWiG are not applicable due to the primacy of the GDPR.²⁵ Due to this position, they often fail to specify in their penalty notices, pursuant to Section 30 (4) OWiG, the member of the executive body or the management person whose culpable action is to be attributed to the company.

¹² *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 8 Rn. 36.

¹³ *Moos/Rothkegel*, in: *Moos*, Datenschutz und Datennutzung, § 5 Rn. 118.

¹⁴ On the concept of undertaking under cartel law, see *CJEU* judgment of 16.3.2004 – Cases C-264/01, C-306/01, C-354/01, C-355/01, para. 46 – AOK Bundesverband and others/Ichthyol-Gesellschaft Cordes, Hermani & Co. and others; see also in: *Bergt*, Kühling/Buchner, GDPR BDSG, Art. 83 para. 40 et seq.

¹⁵ *LG Bonn* ZD 2021, 154 (157) with note by *von dem Bussche*; *Ebner/Schmidt*, CCZ 2020, 84; *Golla*, in: *Auernhammer*, DSGVO BDSG, Art. 83 Rn. 25 f.; *Holländer*, in: *Wolff/Brink*, BeckOK DatenschutzR, Art. 83 Rn. 14.1; *Albrecht/Jotzo*, (footnote 12 above), Rn. 35; *Hohmann*, in: *Roßnagel*, Europäische Datenschutz-Grundverordnung, § 3 Rn. 321; *Roßnagel*, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, p. 134; *Dieterich*, ZD 2016, 260 (265); *Neuhöfer/Schmidt*, jurisPR-Compl 3/2017 note 5; *Rost*, RDV 2017, 13 (16 f.); *Schönefeld/Thomé*, PinG 2017, 126 (127).

¹⁶ *CJEU* judgment of 11.7.2006 – C-205/03 P, marginal no. 25 – FENIN; elaborate on the broad understanding of the *EU Commission* and the *CJEU Cornelius*, in: *Forgó/Helfrich/Schneider*, Betrieblicher Datenschutz, Part XIV marginal no. 90 ff.

¹⁷ *Frenzel*, in: *Paal/Pauly*, GDPR BDSG, Art. 83 Rn. 20; *Faust/Spittka/Wybitul*, ZD 2016, 120 (123 ff.); *Feldmann*, in: *Gierschmann/Schlender/Stentzel/Veil*, GDPR, Art. 83 Rn. 30; *Wolff*, in: *Schantz/Wolff*, Das neue Datenschutzrecht, Rn. 1121; *Piltz*, K&R 2017, 85 (92), also for the English version of the GDPR; *Grünwald/Hackl*, ZD 2017, 556 (558 f.); *Grünwald/van der Wolke/Hackl*, Privacy & Security Law Report, 16 PVLR 1359, 10/9/17, p. 3.

¹⁸ *CJEU* judgment of 19.6.2014 – C-345/13 – Karen Millen Fashions; *CJEU* judgment of 24.11.2005 – C-136/04 – Deutsches Milchkontor; *CJEU* judgment of 25.11.1998 – C-308/97 – Manfredi; *CJEU* judgment of 19.11.1998 – C-162/97 – Nilsson.

¹⁹ *Ebner/Schmidt*, CCZ 2020, 84 (85).

²⁰ *LG Berlin* ZD 2021, 270 with note by *von dem Bussche*, marginal no. 24.

²¹ *LG Berlin* ZD 2021, 270 with note by *von dem Bussche*, marginal no. 23; on this: *Kühn/Sembritzki*, ZD 2021, 193 (194).

²² Different view *Ambrock*, ZD 2020, 492 (493).

²³ *Adelberg/Spittka/Zapf*, CB 2021, 149 (152); also: *Holländer* (see footnote 15), para. 10 ff.

²⁴ On this *Ebner/Schmidt*, CCZ 2020, 84 (85 ff.).

²⁵ *LG Bonn* ZD 2021, 154 with note by *von dem Bussche*; *Bergt* (see footnote 14), marginal no. 20; *Ambrock*, ZD 2020, 492 (496).

However, it is currently highly controversial whether these additional requirements under Sections 30, 130 OWiG are superseded by the GDPR,²⁶ or whether they continue to apply in the case of fines under Art. 83 GDPR with the consequence that the supervisory authority would have to determine a sufficient connecting factor.²⁷

Contrary to the widespread practice of the authorities, it is very well arguable that Sections 30 and 130 of the OWiG are also applicable in the context of Article 83 of the GDPR.²⁸ Pursuant to Section 41 (1) sentence 1 BDSG, the provisions of the OWiG apply mutatis mutandis to violations pursuant to Article 83 (4) to (6) GDPR, unless the BDSG provides otherwise. Only Sections 17, 35 and 36 OWiG are excluded from applicability to violations of data protection law pursuant to Section 41 (1) sentence 2 BDSG. Sections 30, 130 OWiG, however, are not mentioned.

The opinion can also be based on the legislative materials to the BDSG, according to which it was a conscious decision of the German legislator because it did not follow the suggestion of the *DSK* to exclude Sections 30, 130 OWiG in Section 41 BDSG from application to administrative offence proceedings under data protection law.

It must also be taken into account that EU sanctions law as a whole still has a rather fragmentary character. Especially in this area, which is sensitive to fundamental rights, there is a need for clear procedural provisions. This applies all the more in view of the enormous amount of fines possible under Article 83 of the GDPR – especially in the interpretation of the supervisory authorities, which (as shown) base the calculation of fines on the concept of an undertaking under competition law. However, only the OWiG contains sufficient procedural provisions in this regard, so that its applicability in proceedings under Article 83 of the GDPR cannot be waived.

The provisions in §§ 30, 130 OWiG are therefore not superseded by the primacy of European law; they can be based on the opening clause in Art. 83 para. 8 GDPR.²⁹ Here, the GDPR leaves it up to the national legislator to make regulations on the attribution of an infringement to a company.³⁰

Therefore, not only must the charge be sufficiently specified in a penalty notice, but according to section 30 (4) OWiG, the member of the executive body or the management person whose culpable action is to be attributed to the company must also be specified. If a penalty notice does not meet these requirements, legal remedies should be examined.

3. Amount of the fine

Finally, there is also considerable uncertainty as to the amount of a fine that is appropriate and lawful.

The starting point for this is Article 83 (2) of the GDPR, which sets out the legal criteria for imposing fines. Once the decision has been made on the „whether“ to impose a fine, however, there is a great deal of leeway for the discretion of the supervisory authorities regarding the amount of the fine under the fine framework of Article 83 (4) to (6) of the GDPR.³¹

With the aim of somewhat unifying and standardising the authorities' practice of imposing fines in Germany, the independent data protection supervisory authorities of Bund and Länder, which are united in the *DSK*, adopted a concept for imposing fines in proceedings against companies on 14 October 2020.³² The concept only binds the German supervisory authorities and in particular does not apply to cross-border cases. It only applies to companies, but not, for example, to associations or natural persons outside of an economic activity.

In this context, it is highly controversial whether the *DSK fine concept* is really compatible with the statutory assessment provi-

sions in Article 83 (2) of the GDPR – in its ruling on the fine notice against *1&1*, the *Bonn* Regional Court deemed the fine amount determined on the basis of this concept to be disproportionate.

a) Criteria for the imposition of fines

According to the *DSK concept*, the assessment of fines in proceedings against companies is carried out in five steps:

■ (1) First, the company is assigned to a size class: The size classes are based on the total worldwide turnover of the enterprise in the previous year. The size classes are based on the total worldwide turnover of the enterprise in the previous year and are divided into small, medium and large enterprises according to the *Commission Recommendation* of 6 May 2003³³.

■ (2) Afterwards, the average annual turnover for the respective size class is determined: From an annual turnover of more than EUR 500 million, the percentage fine framework of 2% or 4% of the annual turnover is to be used as a maximum limit, so that a calculation is made for the respective enterprise on the basis of the concrete turnover.

■ (3) Subsequently, the supervisory authority determines the so-called basic economic value (corresponding to a „daily rate“): For this purpose, the average annual turnover of the relevant size class in which the enterprise has been classified is divided by 360 (days) and thus an average daily rate rounded up to the pre-decimal figure is calculated.

■ (4) In the next step, this basic value is multiplied by a factor depending on the severity of the offence: Here, the supervisory authorities classify the severity of the offence as light, medium, serious or very serious on the basis of the concrete circumstances of the individual case within the meaning of Article 83 (2) sentence 2 GDPR. Depending on whether formal (Art. 83(4) GDPR) or material (Art. 83(5), (6) GDPR) infringements are involved, different high factors apply in each case.

■ (5) In the last step, the authorities make a correction of the value based on offender-related and other circumstances not yet taken into account: An overall assessment is carried out again, taking into account all circumstances that speak for and against the company, insofar as these have not yet been taken into account under (4). In addition to the criteria according to Article 83 (2) of the GDPR, circumstances such as a long duration of proceedings or an imminent insolvency of the company should also play a role here.

b) Conclusions from the application of the concept of fines in practice

In the meantime, the *DPA fine concept* has already been applied in several proceedings, so that certain practical experience already exists. However, it is not yet sufficiently transparent whether the supervisory authorities apply the agreed criteria in

²⁶ *LG Bonn* ZD 2021, 154 (155) with note by *von dem Bussche*.

²⁷ A good overview of the state of the dispute is provided by: *Adelberg/Spittka/Zapf*, CB 2021, 149 (151).

²⁸ *LG Berlin* ZD 2021, 270 with note by *von dem Bussche*, para. 11, 16; *Popp*, in: *Sydow, DSGVO*, 2nd ed. 2018, Art. 83 para. 5; *Gola*, *Datenschutz-Grundverordnung*, 2nd ed. 2018, Art. 83 para. 11; *Schantz/Wolff* (supra footnote 17), para. 1128; *Taeger/Spittka*, DSB 2020, 292 (293).

²⁹ *LG Berlin* ZD 2021, 270 with note by *von dem Bussche*, marginal no. 16; also *Ambrock*, ZD 2020, 492 (496).

³⁰ *Messner*, ZD 2020, 463 (466); *Popp* (footnote 28 above); *Gola* (footnote 28 above), paras. 11, 16 f.; *Venn/Wybitul*, NSTZ 2021, 204 (209); on the comparable legal situation in Austria: *ÖVGZ* ZD 2020, 463 with note by *Messner*.

³¹ *Holländer* (footnote 15 above), para. 27.

³² Concept of the independent data protection supervisory authorities of the Federation and the Länder on the apportionment of fines in proceedings against companies v. 14.10.2020, available at: https://www.datenschutzkonferenz-online.de/media/ah/20191016_buBgeldkonzept.pdf.

³³ *Commission Recommendation* of 6.5.2003 concerning the definition of micro, small and medium-sized enterprises, 2003/361/EC, OJ L 124, 20.5.2003, p. 36.

the same way. This is unfortunate because decisive aspects remain open; for example, the weighing of the assessment criteria among each other.³⁴ The following initial conclusions can be drawn from the cases of application so far:

Turnover-centred calculation approach

In the event that a company commits a breach of the GDPR, the amount of the fine pursuant to Article 83 (4), (5) and (6) of the GDPR is generally determined by the amount of its „total annual turnover achieved worldwide“. In its concept of fines, the *DSK* even makes the company turnover the lynchpin of the calculation of fines, which in itself is legally questionable from the point of view of proportionality.³⁵ Turnover is not even mentioned as a factor in the calculation of fines in Article 83 (2) sentence 2 of the GDPR.

But also from an economic point of view, the method is not fully developed: A primarily turnover-based fine assessment regularly leads to the fact that a fine for even a minor violation of a high-turnover company can easily reach millions, while even very serious violations of low-turnover companies would be sanctioned with minimum amounts. In such cases, this focus on turnover no longer leads to appropriate results.³⁶ The *Regional Court of Bonn* has already expressly decided this and therefore reduced the fine imposed by the *BfDI* on *1&1* from an amount of 9.55 million euros to 900,000 euros.

Fines based on the *DSK fine concept* may therefore be structurally too high. For this reason alone, an appeal against a penalty notice may make sense, although the circumstances of the individual case must of course be taken into account.

Limitation of the relevant turnover

The authorities therefore have a vested interest in applying the fine concept in such a way that it meets the requirements of the proportionality principle. In order not to be out of line with a blanket reference to the worldwide annual turnover, it happens that supervisory authorities do not necessarily take the worldwide turnover as a basis for calculating the daily rate to be applied for the infringement according to step (3) of the approach; depending on the infringement, there may also be a regional or geographical limitation of the relevant turnover.

This approach is to be agreed with; it is even legally required: Even if – as the *DSK* advocates in its concept – one wanted to base the determination of the relevant company turnover on the antitrust law concept of a company pursuant to Art. 101, 102 TFEU, one would in any case also have to be guided by the standards for the calculation of turnover which are applied by the *EU Commission* and the *CJEU* within the framework of this antitrust law consideration pursuant to Art. 101 and 102 TFEU. These are derived from the Guidelines on the method of setting fines pursuant to Article 23(2)(a) of Regulation No 1/2003 (hereinafter: Guidelines) for the imposition of fines for infringements of Articles 101 and 102 TFEU.

The application of these guidelines has also been approved by the *CJEU* for the determination of the relevant turnover. Accord-

ing to the established case law of the *CJEU*, point 13 of the Guidelines aims to establish as a starting point for the calculation of the amount of the fine imposed on an undertaking an amount which reflects the economic significance of the infringement and the respective weight of that undertaking in it. Consequently, the concept of turnover used in point 13 of the 2006 Guidelines cannot be extended to include sales made by the undertaking concerned which are not covered by the alleged cartel.³⁷

Transferred to infringements of the GDPR, it can be concluded from this that the basic amount to be calculated for a GDPR fine may only represent that part of the turnover that is „covered“ by the alleged infringement. The analogous application of the *Commission's Guidelines* is also particularly obvious here because – in line with the *DPA's* approach to setting fines – it first provides for the determination of a basic amount, which is then adjusted upwards or downwards depending on the severity of the infringement (cf. points 10 and 11 of the Guidelines).

According to point 9 et seq. of these Guidelines, the relevant basic amount (corresponding to the reference value according to the *DSK fine concept*) is determined by the value of the goods or services sold by the undertaking concerned in the relevant geographic market within the EEA which are directly or indirectly related to the infringement (cf. Guidelines, point 13).

This means that the turnover must be limited both geographically and factually in order to determine the basic amount: From a geographic point of view, it has to be determined on which (geographic) market an infringement has an impact. Only the turnover achieved there is likely to be taken into account. In addition, the relevant turnover must also be determined factually; e.g. according to which product or range of services or which group of persons the infringement relates to.

When multiplying the basic value in step (4), the supervisory authorities are apparently mainly guided by the factor pursuant to Art. 83 (2) lit. a GDPR. In some cases, they carry out a separate assessment in qualitative and quantitative terms. Qualitative criteria include the type of personal data and the type of processing, while quantitative criteria include the number of data subjects and data sets. If different factors emerge from these two evaluation dimensions, an average value is then calculated.

When adjusting the basic value on the basis of all other circumstances in favour of and against the data subject pursuant to step (5), the supervisory authorities primarily take into account the other assessment criteria pursuant to Art. 83 (2) lit. b to lit. k GDPR. Initial practical experience shows that the weighting of these criteria is very much dependent on the individual case. Nevertheless, a few general conclusions can be drawn:

- Measures to mitigate the impact and stop a breach, as well as good proactive cooperation with the supervisory authority, can have a strong impact in reducing fines;
- The fact whether the offence was committed intentionally or negligently has a prominent meaning and is attributed more importance in the evaluation than other criteria;
- Reputational damage due to the data breach (or significantly the reporting of it) can also be taken into account;
- It is important to note that an agreement reached with the supervisory authority can also have a substantial effect in reducing the fine because of the acceptance of the unlawfulness expressed in this way.

Whether these attempts to mitigate the relevance of the turnover will save the fine concept is an open question. In the literature, the continued application of the concept is viewed critical-

³⁴ Lang, CB 2020, 20 (22).

³⁵ Classified as „problematic“ by: *LG Bonn* ZD 2021, 154 (158) with note by von dem Bussche; also critical: Lang, CB 2020, 20 (22).

³⁶ Behr/Tannen, CCZ 2020, 120 (124).

³⁷ *CJEU* judgment of 11.7.2013 – C-444/11 P, para. 76 – Team Relocations and others v. Commission, not published, (EU:C:2013:464); judgment of 12.11.2014 – C-580/12 P, para. 57 – Guardian Industries and Guardian Europe v. Commission (EU:C:2014:2363); judgment of 19.3.2015 – C-286/13 P, para. 148 – Dole Food and Dole Fresh Fruit Europe v. Commission (EU:C:2015:184); judgment of 23.4.2015 – C-227/14 P, para. 53 – LG Display and LG Display Taiwan v. Commission (EU:C:2015:258) and judgment of 7.9.2016 – C-101/15 P, para. 19 – Pilkington Group and others v. Commission (EU:C:2016:631).

ly.³⁸ As already mentioned, the *Regional Court of Bonn* also considered the primarily turnover-based calculation of fines, as laid down in the current *DSK fine concept*, to be disproportionate.³⁹ Whether and when an adjustment of the *DSK fine model* will take place, however, has not yet been determined.

III. Conclusion

As far as can be seen, companies in the games industry have so far been spared large GDPR fines. But this does not have to continue forever: Because the data processing of many games companies harbours a certain risk potential, a relevant GDPR violation can certainly result in a hefty fine. However, the receipt of such a fine notice does not necessarily mean that the last fair has been read: The practice of the authorities and, above all, the courts in GDPR fine proceedings shows that the fine notices are not infrequently defective. It should therefore be carefully examined whether and, if so, which deficiencies a penalty notice contains and whether an appeal should therefore be taken.

³⁸ *Adelberg/Spittka/Zapf*, CB 2021, 149 (152); *Taege/Spittka*, DSB 2020, 292 (293).

³⁹ *LG Bonn* ZD 2021, 154 (158) with note by *von dem Bussche*; also critical: *Lang*, CB 2020, 20 (22).

For a quick read ...

- As far as is known, no serious fines have yet been imposed on games companies for violations of the GDPR.
- However, the data processing of many games companies does have a significant risk potential, among other things because of the amount of data, the security threats in the online area (cybersecurity) and partly also the youth of the players.
- GDPR violations and fines as sanctions are therefore quite within the realm of possibility.
- Practice shows that many legal issues surrounding the lawful imposition of fines on companies for GDPR violations are unclear and controversial.
- The DPA concept for the imposition of fines itself also does not appear to be consistently compatible with the GDPR requirements.
- If the worst comes to the worst, it is therefore advisable to carefully consider legal remedies against a penalty notice.



Dr. Flemming Moos

is a lawyer and partner at Osborne Clarke in Hamburg.