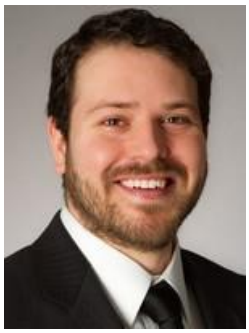
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

GDPR Gameplay: Privacy Issues For Video Game Developers

By **Roger Wylie and Frank Johnson Jr.** (July 5, 2018, 1:33 PM EDT)

Roger Wylie



Frank Johnson Jr.

As the EU General Data Protection Regulation was enacted on May 25, 2018, many organizations such as Amazon, Facebook, Googleand Microsoft were quick to provide updated privacy policies to customers and users in the U.S. and abroad in an effort to conform. Large organizations may have been aware and enacted plans to conform to the GDPR long before the May 25, 2018, deadline, but some smaller entities may have been left with questions regarding how to properly prepare and conform to the new data privacy requirements. One type of smaller entity that this article focuses on is independent video game developers, sometimes referred to as indie game developers, who may collect and utilize data from users to improve their games, add/remove features, or release new content. With this in mind we will first go over some features of the GDPR that are relevant to indie game developers.

GDPR Key Features

Some of the more pertinent GDPR features include: a definition of personal data, a definition of interaction with the EU that is sufficient such that an entity is responsible for or within the scope of the GDPR, penalties for nonconformance to the GDPR, and required consent from users to collect data. Taking each of these in turn, the European Commission describes personal data as "any information that relates to an identified or identifiable living individual," and "[d]ifferent pieces of information, which collected together can lead to the identification of a particular person."[1] The GDPR has increased territorial scope such that it applies to all companies or organizations processing the personal data of data subjects residing in the Union, regardless of the company's location. Further, the GDPR applies to the processing of personal data where the activities "relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU."[2] Entities that do not conform to the GDPR can be fined up to 4 percent of their annual global turnover or 20 million euros, whichever is greater. Finally, consent to collect data from users must be written clearly, gained separately for each term, renewed regularly, and avoid "legalese."

As one can clearly see from just some of the key features of the GDPR, entities that are not prepared may face an uphill challenge in attempting to conform and, worse yet, may face high penalties for a failure to conform. The penalties and multitude of requirements may leave indie game developers anxious as they

attempt to design, code, and implement projects.

Business Issues Faced by Indie Game Developers

A video game developer and/or designer, such as an indie game developer, may run afoul of the GDPR as it attempts to collect data from users interacting with its game in an effort to improve or add new features to said game. As such, the developer may be wary or unsure of how to collect such data while still conforming to the GDPR. A video game developer may wish to collect data from users as they interact with a game in alpha, beta, or final builds to nerf (decrease or reduce the effectiveness of a feature) or buff (increase or improve the effectiveness of a feature). For example, a developer may wish to know how many users utilize a certain type of weapon over another type of weapon in order to apply buffs or nerfs as needed according to collected data.

Developers also utilize collected data to catch hackers (users who utilize third party programs to enhance their own gameplay and obviate boundaries put in place by the developers), cheaters (one or more users that organize groups to artificially increase statistics for a certain portion of users), or trolls (users whose goal is to ruin the experience for other users of the same game). Developers may also utilize collected data to identify areas of games where users spend the most time thereby identifying an indicator for new content such as end game dungeons or multi-party raids in a massively multiplayer online game. No matter the purpose of the data collected by video game developers, there is a potential for the developers and their associated entities to be noncompliant with the GDPR, and therefore subject to its penalties, as some of the users that the data is collected from reside in the EU.

For example, some video game developers may wish to obtain a user's name, address and billing information for business reasons such as enabling in-game purchases or the mailing of physical products and exclusives such as t-shirts or statues of video game characters. Other developers may wish to foster an online marketplace where users can buy and trade in-game products such as character skins to each other, or a gambling scenario where users can pay money for a chance at exclusive items, item skins, or characters. This type of personal data (name, billing information, address, etc.,) could easily fall within the purview of the GDPR as it "relates to an identified or identifiable living individual," or when "collected together can lead to the identification of a particular person." The issue then becomes how can developers, particularly indie game developers, design, implement, and improve their games using data collected from users while still conforming to the GDPR?

Potential Solutions

Indie game developers and developers in general should take heed of the guidance provided by the European Commission by adopting privacy by design, which "calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition."[3] While developing a game, a developer should take into consideration the features it wishes to implement (e.g., marketplaces, gambling, etc.,) as well as the audience that the game will be marketed toward.

Put another way, will the video game be offered via a digital publisher like Valve's Steam platform to an international or worldwide audience? Will the game collect data that could "relate[] to an identified or identifiable living individual," or when "collected together can lead to the identification of a particular person"? If so, a developer should implement clear and concise privacy notices that inform users about how the data will be collected and utilized, and offer opportunities for users to opt-out of certain data collection operations as well as remove data upon request. The developer should ensure that it has identified the legal basis (e.g., consent, necessary for the performance of a contract, compliance with a

legal obligation, legitimate interests, etc.) for each category of processing of personal data and prepare a data processing register that complies with the requirements of Article 30 of the GDPR.

As for collecting data, a potential solution may be to collect and maintain anonymized data in the aggregate such that an individual data point does not relate to anidentified or identifiable natural person or has been rendered anonymous in such a manner that the living individual is not or no longer identifiable. For example, in the item-weapon use case scenario above, user data that is collected on an aggregate level and that indicates overall usage of a particular weapon (as opposed to individual use of weapons by individual users) may suffice to not be considered personal data.

Regardless of which avenue developers decide to utilize when collecting in-game data, indie game developers in particular should attempt to adhere to the GDPR by at least documenting the data it processes that it subject to the GDPR in accordance with Article 30 of the GDPR, providing concise and clear privacy notices, obtaining consent in accordance with the GDPR when necessary, providing removal/erasure procedures, an opt-out feature for collected data, identifying a compliant data transfer mechanism and amending subprocessor/subcontractor agreements as required by Article 28 of the GDPR. Unless all of a user base refuses to allow a developer to collect in-game usage data, then a developer should still be able to collect enough data to develop new features, catch trolls, etc. However, as stated at the beginning of this section, it would behoove indie game developers to be aware of the data privacy concerns brought up by the GDPR at the design stage as opposed to an afterthought.

GDPR Issues for Platforms and Technologies Associated With Video Games

As a small aside, not only should video game developers be aware and attempt to conform to the GDPR but other related entities such as streaming platforms (YouTube's Live) or associated hardware manufacturers (e.g., computer web-camera hardware manufacturers) should also consider the key features of the GDPR. As an example, YouTube Live, which hosts live video streams of users playing video games and streaming such content to computers of tens of thousands of users all over the world, may not edit or otherwise change incoming data from the hosts prior to providing it to users. However, the streaming platform itself may obtain or collect data on its content providers as well as its viewers to obtain viewing statistics, broadcast marketing materials for certain hosts, etc. Such streaming-content entities may need to provide an adequate data privacy policy that conforms to the GDPR as they may collect data in such a way that can be used to identify a user.

Hardware manufacturers of computer webcams may also need to update data collection operations or otherwise adhere to the GDPR. For example, certain webcams may collect geolocation data about users utilizing the hardware. Such data could easily identify a user or, when collected together, can lead to the identification of a particular person. Further, such data may be provided in any captured content via the webcam to a streaming platform such as YouTube Live. In such a scenario, the streaming platform may be required to scrape or otherwise remove such captured geolocation data before it is provided to content viewers to avoid liability under the GDPR or to conform to the GDPR. Moreover, by scraping such data (e.g., streaming data from hosts) prior to providing it to users, entities may further insulate themselves from liability in a swatting incident (making a prank call to emergency services in an attempt to bring a swat police force to a particular address). For example, some users may find it more difficult to engage in swatting if they are unable to scrape the geolocation data from webcams provided via the streaming platform and obtained by the hosts hardware. Similar to video game developers, content streaming entities and computer hardware manufacturers should update privacy policies and inform their user base of the collected data, how it is utilized, and inform users of opt-out features and removal procedures in an attempt to conform to the GDPR.

Roger Wylie is a partner at Kilpatrick Townsend & Stockton LLP and managing partner for the firm's Seattle office.

Frank Johnson Jr. is an associate at the firm.

[1] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

[2] https://www.eugdpr.org/key-changes.html

[3] Id.