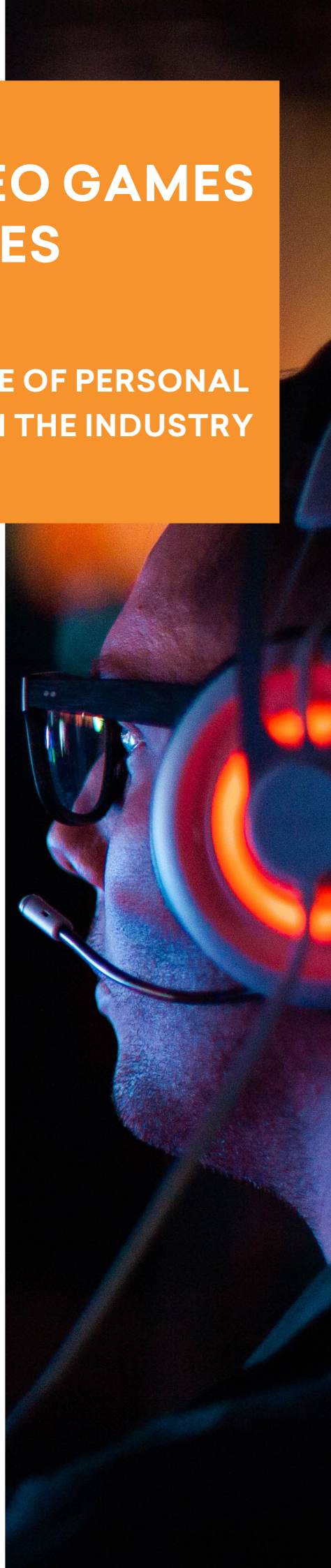
SIMONT | BRAUN

VIDEO GAMES SERIES

THE USE OF PERSONAL DATA IN THE INDUSTRY

Video Games Team | March 2024

The video game industry's increasing reliance on personal data presents a complex legal landscape that game developers must carefully navigate. As the gaming landscape evolves, the role of personal data becomes more pronounced. This article delves into two key aspects: the utilisation of personal data in game analytics and the recurrent theme of data breaches in the sector. In examining these topics, we will explore the legal challenges posed by the General Data Protection Regulation (GDPR).



GAME ANALYTICS

Throughout the last decades, the importance and use of data have known a spectacular increase in most industries - and certainly in the gaming industry. One example thereof is game analytics.

Data 'analytics' refers to the process of discovering and communicating patterns in data, to subsequently inform operational, tactical and strategic business decisions. This requires statistical analysis, data mining and forecasting, mathematics, etc. Applied in the context of game development, these processes are referred to as 'game analytics'.

Specialised literature differentiates 4 use cases for game analytics: game analytics used as (i) a sense-making tool, allowing understanding player behaviour, (ii) a decision-support system, where data is used to answer strategic business questions, (iii) a communication tool, used to inform investors and publishers, and better justify decision made, and (iv) a 'hygiene factor', allowing 'serious' and more 'mature' companies to continuously improve their products and stand out from the average[1].

The challenges that game analytics present from a GDPR perspective are various.

Security of the data - As game analytics involves the storage and analysis of large volumes of data, ensuring the security and protection of those data becomes paramount. Companies failing to implement robust cybersecurity expose themselves to many risks, including legal ones, and especially when their failure to protect the data leads to a data breach (see below the legal implication of data breaches). Regulatory bodies and users are increasingly holding companies accountable for such breaches, and failure to protect personal data can result in severe fines as well as reputational damage.

Legal basis for processing - Any processing of personal data must have a valid legal basis. Given the type of processing involved in game analytics, it generally goes beyond what is necessary for the performance of their contractual obligations, leaving them with only two legal bases, being (i) the gaming company's legitimate interest and (ii) the clear and informed

1. M. Mäntymäki, S. Hyrynsalmi & A. Koskenvoima, « How Do Small and Medium-Sized Game Companies Use Analytics? An Attention-Based View of Game Analytics », *Inf Syst Front 2020*, 1168-1173.

consent from the data subject. The available legal bases would be even more limited if the data used in the data analytics are considered as biometric data, as those cannot be processed based on the basis of the legitimate interest of the gaming company.

For those data as well as other data for which no legitimate interest to the processing has been identified, gaming companies should capture their user's consent to the intended processing. When doing so, gaming companies should design user interfaces that effectively communicate the data practices to users and obtain their explicit consent in a compliant way. Additionally, companies need to provide users with the option to opt out of data collection without compromising their gaming experience.

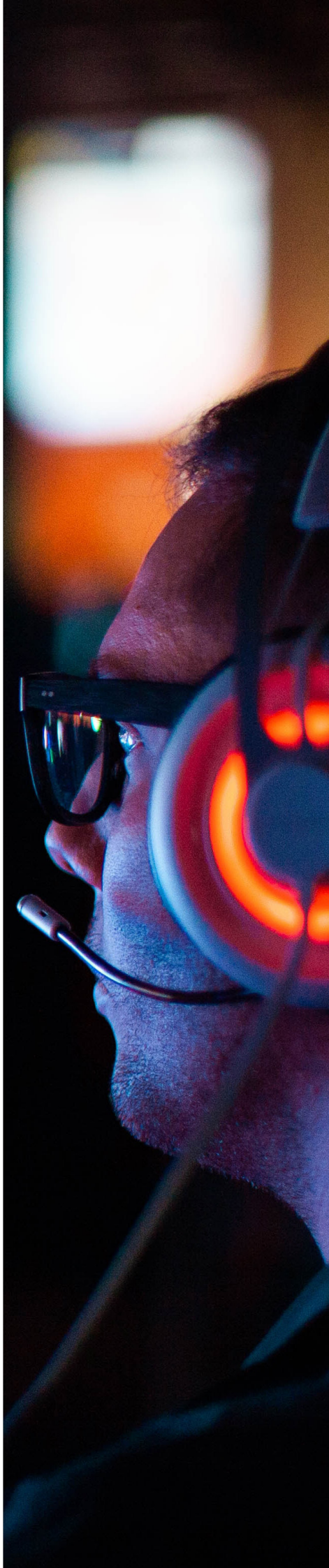
Transparency - Companies must provide transparent information to the data subjects to inform them 'in a concise, transparent, intelligible and easily accessible form' on the intended processing. This includes the processing in the context of data analytics, which must be easily understood by the data subject. Legal issues emerge when companies are not transparent about their data practices or when users feel coerced into consenting to certain data processing they may not fully understand.

Impact assessment – When companies identify that certain processing activities are likely to create high risk for the rights and freedoms of individuals, they have the obligation to conduct a more in-depth impact assessment of the processing concerned. This data processing impact assessment should allow for a better understanding of the actual risk of the processing. Depending on the outcome of the assessment, companies may be required to implement additional security measures to reduce risks. In cases where companies are not able to reduce risks below a high risk, prior consultation of the competent data protection authority is required before any processing activity takes place.

Automated processing – Depending on the particular processing, game analytics may lead to automated decision-making. In such a case, GDPR imposes restrictions on such automated processing to protect individuals' rights. Game developers must ensure that automated decisions are necessary for contracts, authorised by law, or based on explicit consent. They must also provide measures for individuals to intervene, express their views, request human intervention and contest decisions. As always, users should be clearly informed of such practices.

DATA BREACHES IN THE SECTOR : A RECURRING THEME

One of the most recent data breaches reported in the gaming industry dates back to December 2022, when *Activision* confirmed that hackers compromised the company's internal servers. *Activision's* response was quick, asserting that no game code, sensitive employee data, or player details had been accessed. Yet, claims to the contrary soon emerged: security research group *vx-underground* mentioned the exfiltration of sensitive workplace documents and content release schedules. Not much later, it became apparent that the data leak involved names, email addresses, phone numbers, salaries, and other critical employee details. This incident illustrates a growing concern in the gaming sector: the disparity between company claims and the actual extent of data breaches. Legal implications arise when companies understate, in case of a data breach, the degree of exposure or when they fail to notify affected parties promptly.



Recent events have shown that *Activision* is not the only victim of attacks. Gaming companies appear to be prime targets due to the large amount of data they process ranging from employees' data to confidential game content over players' data, which in turn can be explained by the growing importance of game analytics. Throughout the last years, other major actors of the industry such as *Riot Games*, *Rockstar Games*, or *Roblox* have disclosed data breaches involving theft of source code, confidential development footage and/or sensitive users' information.

As point out earlier, the first obligation when it comes to data breach is for the data company to take all appropriate security measures to protect personal data. However, even when using best industry practices in terms of security, the risk of a data breach happening cannot be eliminated.

When a data breach occurs, companies are legally obligated to disclose the incident promptly and accurately to their data protection authority. To avoid unjustified delay in this reporting, and thus any potential fine, companies should make sure they have efficient and robust reporting and incident response plans to investigate, address and report the breach promptly. In the gaming industry, where sensitive player information is at stake, the timely and accurate disclosure of data breaches is crucial as it is likely that the breach might result in high risk to the rights and freedoms of data subjects. In such case, companies must also inform data subjects of the breach.

Post-breach, gaming companies must be ready for potential investigations by regulatory authorities. GDPR compliance is therefore essential not only in preventing breaches but also in responding appropriately when they occur. Companies must adhere to legal requirements for reporting, cooperating with investigations, and implementing remedial measures. Failure to comply with these post-breach obligations can result in additional sanctions.

WHAT ARE THE RISKS OF NON-COMPLIANCE ?

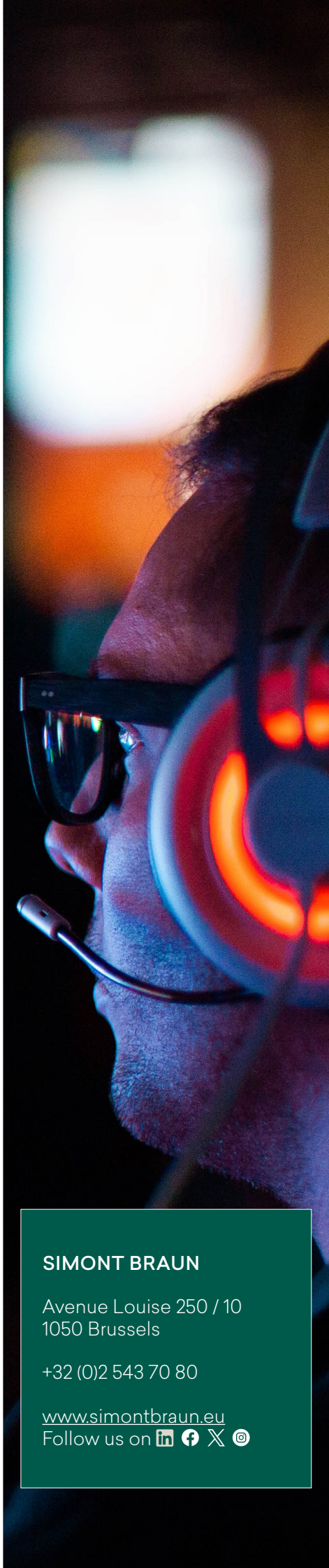
Risks related to GDPR non-compliance are multiple ranging from reputational damage to fines. Indeed, failure to comply with any GDPR related obligations may result in heavy fines imposed by the local data protection authority after investigation. Individuals affected by the non-compliance may also take legal action if they perceive that a company has been dishonest or negligent in its reporting.

CONCLUSION

For game developers, the intertwining paths of innovation and legal compliance are complex but unavoidable. Navigating the GDPR maze might seem daunting for gaming companies, especially with such high stakes. Yet, with proper understanding and implementation, it's a navigable challenge.

For any questions or assistance, don't hesitate to email our Video Games Team at gaming@simontbraun.eu.

This article is not a legal advice or opinion. You should seek advice from a legal counsel of your choice before acting upon any of the information in this article.



SIMONT BRAUN

Avenue Louise 250 / 10
1050 Brussels

+32 (0)2 543 70 80

www.simontbraun.eu
Follow us on