

Spain and Belgium publish joint European guidance on data protection in video games

IRIS 2026-9:1/26

*Joan Ramon Rodriguez-Amat
European Audiovisual Observatory*

The "Recommendations and best practices for personal data protection in video games" are the first joint European guidelines dedicated exclusively to addressing data protection, user privacy, and systemic risks within the video games ecosystem under the General Data Protection Regulation (GDPR). They have been published collaboratively between the Spanish Data Protection Agency (*Agencia Española de Protección de Datos* - AEPD) and the Belgian Data Protection Authority (*Autorité de protection des données* (APD) / *Gegevensbeschermingsautoriteit* (GBA)).

Grounded in the principle of privacy by design and by default, the document is an effort to translate high-level GDPR obligations into actionable, operational guidelines for developers, studios, publishers, hardware providers, and digital distribution storefronts across all development and operational phases. The publication thus addresses the technological complexity and massive processing operations inherent in modern video games. It assumes that compliance in interactive software cannot be achieved retroactively because structural software architecture, database design and interface mechanics constrain data flows permanently; because of that, the principle of privacy by design (Article 25 GDPR) must serve as the primary framework for game governance. Accordingly, establishing a data controller, and data processor relationships between hardware vendors, engine providers, developers and platform distribution stores is a vital condition prior to launch. Similarly, early governance intervention ensures that any forms of automated profiling – including algorithmic difficulty adjustments or large-scale telemetric logging – remain fully compliant with legal bases, data minimisation and purpose limitation requirements at all times.

The guidelines draw attention to a structural vulnerability in gaming: the immersive, fictional nature of interactive environments often induces a false sense of anonymity among players, obscuring the reality of continuous data collection. In order to prevent this, data controllers are expected to provide clear,

layered, and granular privacy information that avoids vague justifications such as "improving user experience" or "supporting advertising services". Instead, games must explicitly clarify legal bases, retention windows and any form of third party data sharing.

The document uses a practical approach and is structured along three operational building blocks:

- 1) Industry mapping and data processing categories: the guidelines provide an overview of the complex multi-stakeholder ecosystem and a map of the data categories processed within the digital interactive entertainment sector.
- 2) Threat and risk identification: the document offers a detailed examination of dark patterns, player opacity, manipulative design practices, and specific vulnerabilities affecting minors.
- 3) Phase-by-phase recommendations: using a comprehensive compliance catalogue helps to check every step in the video game lifecycle: pre-production, production, launch and post-production.

The guidance provides methodological tools, interactive questionnaires, self-assessment checklists and analysis of data controller and processor roles at each stage of a title's lifecycle to clarify responsibility in multi-layered processing chains.

The guidelines highlight three major, high-risk categories of personal data processing that require more heightened regulatory scrutiny than the basic account registration data (usernames, email addresses, and passkeys). These categories include:

- account creation and identity management (identifiers provided by the direct user during onboarding and authentication);
- telemetry and in-game monitoring (involving background data point logging – at rates of dozens per second – that includes micro-interactions, session lengths, character movements, text and voice logs in-game, or even biometric identifiers like voice telemetry, facial expression tracking and eye movement data); and
- behavioural inferences for personalisation and monetisation (using AI and machine learning to generate profile data that evaluates dynamic gameplay logs and constructs detailed psychological profiles that predict user skills, engagement drop-off points, consumer and emotional vulnerabilities).

The guidance also rigorously defines and prohibits manipulative design patterns by entering the key space between user experience (UX) design, consumer protection and data privacy. This involves dealing directly with dark patterns,

addictive mechanics, and loot boxes.

The text establishes a regulatory stance of presumption of the presence of minors that assumes that children constitute a portion of the gaming demographic and that they face risks regarding profiling, commercial exploitation or peer harassment. This stance applies by default unless the video game can provide verifiable proof that its content and target audience are exclusively restricted to adults. The consequence of this is that studios and publishers must default to the strictest privacy configurations (privacy by default) which means disabling commercial profiling, personalised monetisation mechanics, targeted advertising, and location tracking for all default profiles, as well as implementing robust, privacy-preserving age-assurance and verification mechanisms.

Directive 95/46/EC (General Data Protection Regulation)

<http://data.europa.eu/eli/reg/2016/679/oj>

Recommendations and best practices for data protection in video games

<https://www.dataprotectionauthority.be/publications/recommendations-and-best-practices-for-data-protection-in-video-games.pdf>

