agencia española protección datos

Autorité de protection des données
Gegevensbeschermingsautoriteit

Recommendations and best practices for data protection in video games.

June 2026

CONTENTS

1. Introduction

1.1 What is a video game?

A video game is an interactive digital experience in which one or more players engage with virtual environments through a system of game rules, objectives, and feedback, typically using electronic devices such as computers, consoles, smartphones or cloud platforms. Video games may incorporate visual, auditory, narrative, and multiplayer components, allowing for competition, collaboration, exploration or creativity. The scope of what qualifies as a "video game" has evolved beyond traditional formats due to new technologies and user experiences.

A video game today can include these traditional video games played on consoles, PCs, or handheld gaming systems and typically offering complex graphics, objectives, and multiplayer or campaign modes. But also, mobile games played on smartphones and tablets including casual at-your-own-pace games and fast-paced multiplayer experiences. There are cloud-based or streaming games delivered via the internet, removing the need for local hardware performance and accessible across different devices (phones, smart TVs, browsers). There are also browser games, web-native (HTML5/JavaScript) and supporting player-created experiences. In a broader sense, there are user-generated environments and game platforms where players become creators, building and sharing their own games and interactive worlds. This model blurs the line between player and developer.

In addition, we need to consider Virtual Reality (VR) and Augmented Reality (AR) games played with headsets or AR-enabled devices that offer immersive environments or overlays on the real world. Furthermore, serious games and highly gamified experiences (interactive training simulators, learning apps) are designed for education, training, learning, health, therapy, or awareness, but still classified as video games due to their interactive and rule-based structure. Finally, in the short term we will likely find in the market AI-driven (Artificial Intelligence driven) and procedural games including autonomous AI characters, dynamic narratives, or generative content. Expectations are to create procedural environments that change each playthrough.

To summarise, the key elements that define a video game today are:

- **Interactivity:** The user performs actions that produce effects or responses.
- **Digital interface:** They are played via a digital platform (not board or physical-only games).
- **Rules and objectives:** They are structured around goals with failure/success criteria and game logic.
- **Feedback system:** There is a real-time response built on visuals, sounds, scores, progression, etc.
- **Entertainment focus:** They are primarily built for fun, challenge, creativity (even if used for education).

1.2 Taxonomy of video games

As introduced before, the video game ecosystem is incredibly diverse, ranging from simple mobile games to complex titles, which makes establishing a single definition difficult and may benefit from segmentation.

A taxonomy, or systematic classification, of video game types can be established by attending to different dimensions and characteristics. These map very naturally onto data protection threats and risks, because each dimension or characteristic tends to change what data is collected, why it is collected, who receives it, and how intrusive the processing is. The more a game is, for example, online, cloud-based, personalised, or monetised through ads and microtransactions, the higher the risk for data protection. This document focuses on those with the greatest impact on data protection (see Table 1).

Dimension	Category	Explanation
Focus	Entertainment	Games focused on providing fun, enjoyment, and stress relief. Entertainment games aim to engage players through elements such as interactive storytelling, art or music.
	Educational	Games designed to improve cognitive, social, and academic skills. They are designed to enhance learning by blending pedagogy with technology.
	Serious games	Games used for serious purposes that extend beyond mere entertainment, often used to train individuals or groups. These games very often model real-world physical activity, environments, or complex systems (simulation tools), enabling users to practice critical tasks or to rehabilitate. This includes uses across domains such as business, health care, transportation (flight simulators, for example) or safety.
Connectivity (often related to the dimension Number of players/player mode)	Offline gaming	Games functioning independently of continuous Internet streaming, though they may use the Internet for updates, sales, or community and social functionalities.
	Online gaming	Games heavily relying on continuous Internet streaming. These games leverage network connectivity to facilitate competition, cooperation, and social interaction among players: multiplayer games, Massively Multiplayer Online (MMO/MMORPG) games. They often require centralised servers for persistence.

Dimension	Category	Explanation
Technological platform	Local device	Games primarily accessed and played directly on dedicated, user-owned hardware (console, PC, mobile phone, etc.), often relying on physical or digital ownership.
	Cloud/streaming gaming	Games streamed directly from remote servers to users' devices, bypassing the need for powerful local hardware.
	Virtual reality and metaverse integration	Games using highly specialised hardware (such as head-mounted displays) or pervasive online infrastructures that create immersive, interactive, and persistent shared virtual spaces, going beyond traditional experiences.
Economic model and monetisation strategy	One-off purchase	This model is the traditional ownership-based one, it involves a single payment (physical or digital) where the consumer acquires and perpetually owns the game. The initial costs for these titles are typically high but grant lifetime access.
	Subscription model	In this model, users pay a recurring fee for access to a single game or a curated, and often rotating catalogue of games (or parts of games), accessible on local devices (purely in-game interface) or via cloud/streaming (platform stores, launchers and storefronts, etc.).
	Free-to-Play (F2P)	This model allows players free access to the game, which generates revenue through microtransactions (small, optional purchases for digital goods and services made inside the game, such as in-game currencies, power-ups, or cosmetic items), in-game advertising (revenue is generated by displaying commercial messages or advertisements within the game environment), or other monetisation methods (loot boxes, battle passes, etc.). F2P relies heavily on player retention to drive long-term monetisation.
	Freemium	This model is based on a blend of free and premium content, offering free access to the game but charging for enhanced features (which can include one-off payments or subscriptions).

Table 1. Video games taxonomy

1.3 Video games lifecycle and industry roles

The video game ecosystem consists of key roles and actors contributing to game creation, distribution, marketing, and consumption. In general, we can find the following roles summarised in Figure 1.

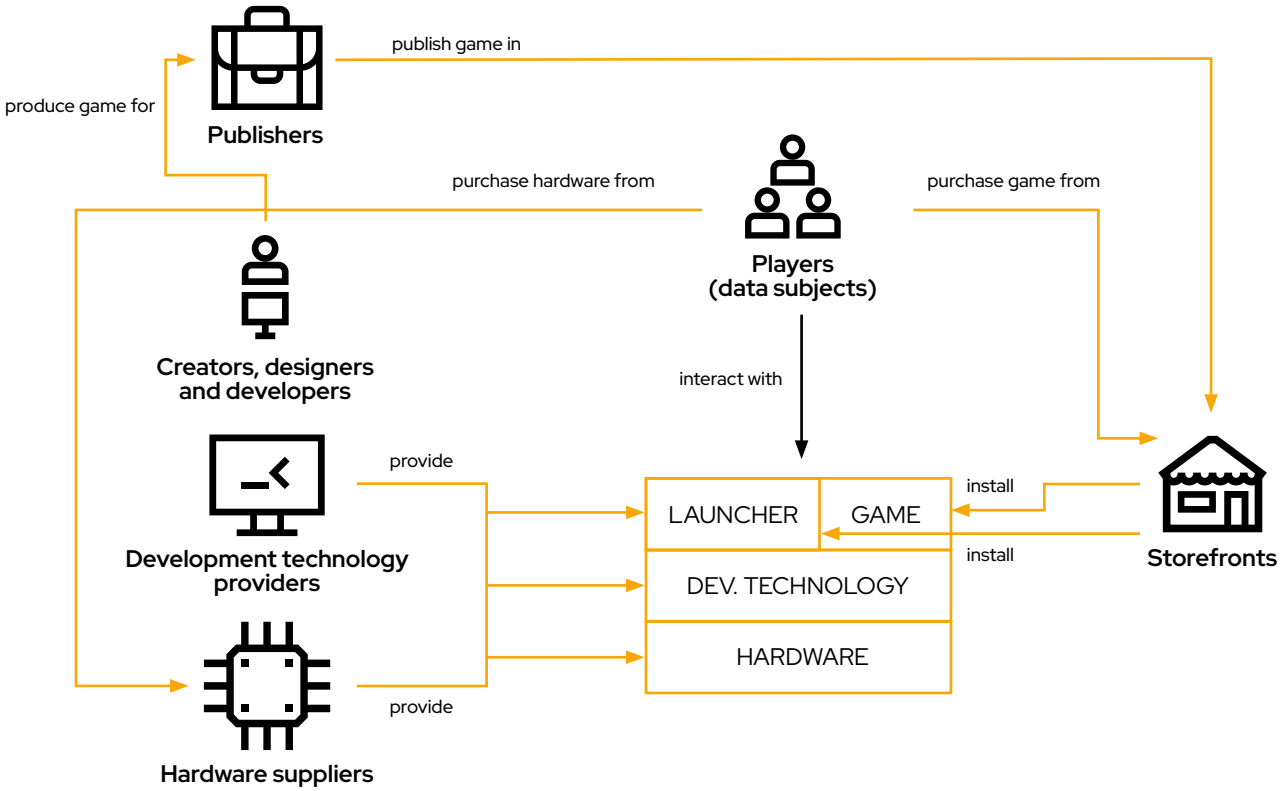

Figure 1. Generic representation of the video games ecosystem and industry roles

1. **Hardware suppliers** provide physical devices that enable gaming. This includes console manufacturers, as well as PC hardware companies that produce essential components such as graphics cards or specific peripherals. These suppliers create platforms and system-level components (hardware drivers, network stack, etc.) on which games run, controlling licensing, platform access, and sometimes charging other actors' royalties for using their hardware.

2. **Creators, designers and developers** are responsible for the actual creation and production of video games. They may be individuals or teams within development studios who design, program, and assemble the elements that make up a game. Developers specialize in various aspects, including game design (defining gameplay mechanics, storylines, and characters), programming (coding game functionality and mechanics), and art creation (visuals, animations, and assets). There are different types of developers based on their relationship with hardware manufacturers and publishers. First-party developers are typically in-house teams owned by console manufacturers, and they mainly develop games exclusively for their respective platforms. Second-party developers are independent studios that have exclusive contracts to develop games for a specific platform holder but retain some independence. Finally, third-party developers (the only ones shown in figure 1 for simplicity's sake) work for external publishers and may develop games for multiple platforms, often governed by contracts with strict milestones and publisher oversight.

3. **Development technology providers** supply the software tools (runtime libraries, middleware, Software Development Kits or SDKs, Application Programming Interfaces or APIs, code packages, engines) that enable game creation and execution. Their products interface directly with hardware suppliers to maintain compatibility, while game creators depend on them for streamlined development. These tools support publishers and developers by easing production and execution challenges across teams and platforms.

4. **Publishers** finance, market, distribute, and sometimes commission games. They coordinate closely with developers and studios to manage production and ensure games meet platform requirements set by hardware suppliers. Publishers negotiate access to storefronts for distribution and oversee market readiness, thereby connecting the creative and commercial aspects of the gaming industry.

5. **Storefronts** are the distribution platforms where players buy or download games, acting as intermediaries between publishers, hardware platforms, and gamers as end consumers. They work with publishers to host and promote games, comply with hardware supplier standards, and ensure that players receive updates and support, thereby completing the distribution chain. Some storefronts focus on a single publisher's catalogue, while others aggregate games from many developers for broader discovery and access. Launchers are strongly related to these storefronts. A launcher is a dedicated application that acts as a centralised hub for buying, downloading, installing, updating, and playing games. Launchers streamline the process of managing large game files, applying updates, and keeping all games organised in one place, rather than requiring players to manually find and install patches or manage separate installation folders for each game. In addition, many launchers offer community features, such as chat, forums, multiplayer matchmaking, and achievements, helping create a richer game experience and connecting players.

This ecosystem operates through constant interconnections among roles. Hardware suppliers establish standards that development technology and developers must satisfy. Developers and publishers collaborate to deliver compelling products, while storefronts ensure games reach players on various platforms. These overlapping relationships form a robust and dynamic system that drives the global video game industry.

It is worth noting that player communities may enrich video games by creating user-generated content (UGC) such as skins, scenarios, mods, and maps, effectively taking on roles as creators, designers, and developers alongside their primary player role. As a result, essential games are not fixed developer products but collaborative ecosystems where players co-author the experience. This dynamic is not unusual, as actors often play multiple roles within the ecosystem. It is quite common for the same company in the video games ecosystem to hold multiple roles simultaneously, especially among larger companies or diversified businesses. Large companies or publishers often act simultaneously as developers, publishers, and sometimes even storefront operators or development technology providers. Hardware suppliers also provide development technologies, such as proprietary engines or SDKs, thereby playing a dual role as both hardware and development technology providers. They can even operate their own storefronts and launchers, that is the case, for example, of the major console manufacturers.

There are different models and frameworks that review the industry practices to identify between four and seven stages involved in video games development. The video game lifecycle or the Game Development Software Engineering (GDSE) process life cycle often diverges from traditional software development methodologies due to the inherent diversity of requirements introduced by creative arts disciplines.

Most conceptualisations of the video game lifecycle feature the three major, macro-level phases summarised in Figure 2.

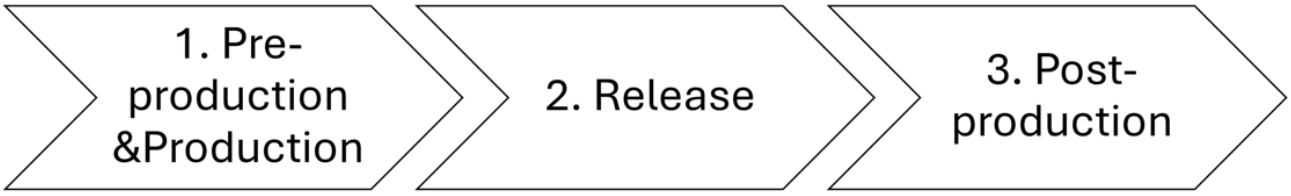

Figure 2. Video games lifecycle

1. Pre-production&Production

- Initiation/Pitch/Concept: This step marks the initial stage where ideas are brainstormed, and concepts and designs are described. It involves defining major game characteristics, such as genre or core mechanics, to produce a rough concept or high-level design.

- Pre-production: This step focuses on planning and preparation, often culminating in the creation of a detailed game design document. Activities include creating storyboards, building prototypes, and confirming internal structures. It typically ends with a playable prototype (or vertical slice[1]) used to secure funding for the completion of production.

- Production: This step focuses on the implementation of game concepts, formal details, refinement, and technical and artistic development (asset creation, source code, integration aspects). This is very often the most time-consuming part of the process.

- Testing: This step involves identifying and fixing bugs, glitches, exploits, and soft locks. It is also used to test the usability, fun factor, and user engagement of the game. Testing outputs help determine whether to proceed to launch or revert to production for refinements. This step is very often concurrent, it can be done during production from the early design steps, as bugs found later are much more expensive to fix.

- Alpha/Beta/Pre-launch: This step involves making the game available to testers (internal or third-party) to check for bugs and gather feedback on a larger scale. The Pre-launch stage includes initial marketing and public awareness campaigns to advance to the next phase.

2. Release

This is the public release of the game, so players can play. It includes giving the game its final polish, quality improvements, and final artistic touches, as well as creating proper documentation and planning for post-launch activities.

[1] A vertical slice is a small, polished section of the game that shows how the final product will look, sound, and play. It includes all the main layers of the game experience, but only for a limited part of the game.

3. Post-production

This is the final stage, crucial for maintaining sustainability. Activities include bug fixing, providing gradual updates and Downloadable Content (DLCs), and marketing. Video games are noted for having a longer monetisation cycle, and the post-launch phase supports continuous engagement, providing exposure that can lead to sales.

It should be considered that this 3-phase model is well-suited for traditional games sold as a one-off purchase but is less applicable to Free-to-play or Freemium games, where most production (development) work occurs after the product is released. It is also worth mentioning that Creators, designers and developers are primarily involved in Phase 1 while Publishers and Storefronts have a major role in Phases 2 and 3.

1.4 Video games and the GDPR

The video game sector is a major global economic force in 2025, with estimated annual revenues approaching $200 billion. This positions it larger than both the film and music industries. The industry continues to expand, driven by over 3 billion gamers worldwide and rapid innovation in areas such as cloud gaming and AI. The sector supports hundreds of thousands of jobs directly and indirectly. It contributes significant tax revenues and fosters innovation in technology, media, and marketing globally. Now, 95% of game sales are digital, reflecting the mainstream move away from physical distribution. This shift boosts online platforms and services, encouraging the development of new business models, such as those based on subscription or digital marketing.

For the purposes of the GDPR[2] (General Data Protection Regulation), personal data means "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" and processing means "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

Therefore, video games process personal data and all the actors involved in the provision of video games must comply with the GDPR principles and requirements when conducting these data processing activities falling within this regulation's material and territorial scope. Processing personal data in video games goes beyond traditional records such as names or email addresses; it includes any information that distinguishes one individual player from others in the game's context, enabling targeted actions, interactions, or differential treatment. This "singling out" triggers GDPR protections because it allows the game to treat that specific person uniquely. Furthermore, automated decision-making and profiling build directly on the concept of singling out individuals, as they involve using personal data to analyse or predict player behaviour and then act on it automatically without human intervention.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Clear specific recommendations on how to comply with the GDPR are essential as the video game industry handles large volumes of personal data, often highly sensitive because it regularly processes information about vulnerable users, including children, and may also collect or infer special categories of personal data such as health data, biometric data, or other data revealing sensitive characteristics. In addition, the processing performed is often high-risk because it involves large-scale, sensitive data, as well as systematic and extensive evaluation, including profiling and automated decision-making, to mention only a few examples. Therefore, because of its nature, scope, context, or purposes, it is likely to create significant threats to individuals' rights and freedoms. Focused guidance clarifies obligations, builds trust among stakeholders, and raises awareness. Data protection risks compromise user privacy, safety and, in general, rights and freedoms. Furthermore, this may undermine the companies' stability through penalties and reputational damage.

1.5 Scope of this document

This document provides GDPR compliance recommendations specifically targeted for professionals and organisations involved in the video game ecosystem. It focuses on legal, organisational, and technical practices for designing, developing and providing entertainment video games, guiding teams to data processing activities within their titles that meet GDPR principles and requirements throughout the game's lifecycle.

2. Personal data processing within video games

Personal data processing in video games covers many activities. These include collecting personal data to create and manage accounts, gathering telemetry on player inputs and actions, and making behavioural inferences for personalisation and monetisation. All of these happen within the complex ecosystem of actors described previously in this document.

Video games process different kinds of personal data. Direct identifiers clearly link to a known person, such as usernames, email addresses, account IDs, or full IP addresses. These let publishers contact people, let them log into a storefront, perform financial transactions, or let one player friend another, like adding "PlayerX" in a game lobby. They also make main features work, such as saving progress or tracking leaderboards.

Pseudoidentifiers replace this direct information with substitutes that still uniquely identify a player, such as device IDs, advertising IDs, session tokens, or hashed combinations (for example, username + timestamp). A pseudoidentifier cannot be attributed to a specific person without additional information kept separately. In games, for example, a persistent player UUID (Universally Unique Identifier) that tracks players across sessions without revealing their name or other identifiers, for example, allowing anti-cheat systems or personalised loot to target "that specific individual" in a multiplayer crowd.

Finally, metadata refers to data that provides information about other data or events within the game environment. It describes attributes, activities, or occurrences, such as timestamps, geolocation pings, logs of mouse movements, crash data, or in-game events like kills and purchases, without directly naming or explicitly distinguishing individuals. However, metadata becomes personal when

linked to an identifiable context. For example, “Player at IP 1.2.3.4 killed enemy at 14:32” combines metadata with an identifier. Even anonymised play patterns (like a “unique sniper headshot rhythm”) can single out individuals when analysed using behavioural fingerprinting.

This section outlines key processing activities, related data types and elements, and prevalent purposes. All considered processing activities involve identifiers, pseudo identifiers, and metadata in addition to content and communication data, financial and transactional data, sensor data, location data, etc. as it will be discussed in the rest of this section.

2.1 Account creation and management

The creation of an account, along with subsequent identification and authentication processes, represents a fundamental personal data processing activity within video games. This step is usually mandatory for users to access key services, especially in online and cloud/streaming games.

Account creation involves the direct and explicit collection of personal data from the user (the data subject) to create a persistent digital identity. The initial registration stage involves collecting data that may be required or optional: the essential information needed to establish the user’s online identity and facilitate security (IAAA for Identification, Authentication, Authorisation and Accountability), but also to enable personalised features. Furthermore, games often encourage or reward players for keeping their account information updated or complete, and for linking their accounts with third-party social networking platforms, which allows the game to access additional personal data governed by the external platform privacy settings. Additionally, the information associated with the accounts can be enriched over time with logins (or attempts) or other security-related aspects.

Data type	Specific data elements
Fundamental data	Name (first and last name) Email address Account name/Username Password Phone number Postal address
Demographic data	Age/date of birth Gender Country Language
Biometric data	Voice sample Face image
Third-party data	Social media account details and handles Contact lists or social graphs

Data type	Specific data elements
Technical information	Preferences and settings
Payment data	Credit or debit card details Billing address Purchase history
Security and safety data	Login logs Authentication tokens Suspicious activity markers Ban history Anti-cheat mechanisms
Parental control	Parental consent records Limited gameplay settings Contact & personal details of parents/guardians

Table 2. Personal data processed for account creation and management

All this data can be grouped into several categories summarised in Table 2.
The processing of personal data for account creation and management is carried out for several purposes, many of which may be necessary for the performance of a contract (i.e., enabling gameplay and service delivery):

- Account creation and access: To create service accounts and allow users to access the services. Registration can be mandatory or optional at different levels (storefront, publisher, hardware supplier) depending on the game and its characteristics. Users are highly encouraged to register and become members, as they may not be able to access key services otherwise.
- IAAA (Identification, Authentication, Authorisation, and Accountability): To verify the user's identity and protect the security of the services and users
- Personalisation and customisation: To create user profiles and offer customised content, which can make the game more engaging. The account information may help the different actors understand player types.
- Connection with peers: To establish social interaction and connect users with other players in multiplayer online games.
- Customer support and dispute resolution: To provide technical support and respond to user inquiries, resolve disputes, and enforce agreements.
- Fraud prevention and safety: To conduct liveness detection, to prevent fraudulent transactions, including the enforcement of the terms of service, and to protect specific individuals or groups.

2.2 Gameplay monitoring (telemetry)

Personal data processing in video games relies heavily on a specific kind of monitoring, often referred to as telemetry, which continuously records player behaviour and performance metrics. Almost all modern gaming stacks (devices, development technology, game, launcher) are designed to transfer behavioural data to remote servers over the Internet. This activity can extend over time, recording actions, decisions, communications, etc. usually with dozens of parameters and signals captured per second.

Video games are unique environments, sometimes considered “rich natural laboratories”, where player behaviour can be intentionally triggered and monitored under controlled conditions, making all the collected data highly sensitive. In this case the data collection is implicit and passive, often completely invisible to the ordinary user. Players are frequently unaware of the nature and amount of data collected and processed about them.

There are some extended methods to process telemetry within games. The first method is using embedded event tracking analytics services. Most games integrate SDKs from analytics providers that let developers instrument custom events (for example, “level_start”, “ability_used”, “shop_visit”). These SDKs bundle telemetry into small packets and send them asynchronously to external endpoints, where they are stored in data warehouse systems for later analysis.

The second method is client and server side logging. Games can log telemetry directly on the game client (JSON or binary logs of sessions, inputs, or errors) and upload them periodically or on crash; server side telemetry is often richer, as authoritative servers see all player states, positions, and interactions without potential client side tampering. Online multiplayer titles often stream structured events (play style, spawns, deaths, chat flags) to a central analytics backend, enabling real time dashboards and fraud or cheat detection.

The third method relies on remote telemetry APIs and UDP streams. In simulation or racing titles, for example, engines expose real-time telemetry data (position, speed, lap times, car state) via these APIs or streams at high frequency. Third party tools (on screen dashboards, racing sim coaches, etc.) consume this stream over the network, treating the game as a telemetry source feeding external monitors rather than only internal analytics.

Finally, sampling and remote config driven instrumentation reduce bandwidth and storage. Some games use these strategies, logging only a representative subset of frames or sessions. Remote configuration lets developers remotely enable or disable specific events, increase logging depth for certain regions or player segments, or tune parameter values without a full patch, which is useful for A/B testing gameplay or financial parameters optimisation.

However, there are many other specific methods for collecting and processing this kind of data. For example, through direct feedback (questions, polls, surveys) and NPCs (Non-Player Character) or AI driven NPCs.

Data processed with all these different methods can be summarised as shown in Table 3.

Data type	Specific data elements
In-game actions	Duration, frequency, direction, strength, speed, or accuracy of a player's interaction Character actions such as movement/navigation, combat actions (shot, kick, punch, block), and interaction with objects/items (collect, drop, use, open/close)
Achievements and game progression	Game level Trophies Ranking Unlocked content
Statistics	Points, lives, scoring In-game currency balance Performance figures, error rates, completion times for tasks
Playtime	Logins (time, length) Gaming frequency Pauses, absence times
Avatars	Profile Features and modifications, skins
Game logs and recordings	Actions taken on games and websites Archives recording chat text and voice communication User-generated content, forum posts
Biometric data	Facial feature points, facial expressions and action units (eyebrow lift, for example) Pupil dilation Eye-movement patterns Head pose Body-movement patterns Brain-related information and patterns Galvanic Skin Response (GSR) and sweat Heart rate Breathing Voice pitch and volume
Technical information	IP address Device type/model, hardware specifications Operating system Connection quality Geolocation

Table 3. Personal data processed for gameplay monitoring

The processing of gameplay data may serve different purposes:

- Game enhancement and technical improvement: Telemetry data is used to enhance game quality. Developers track player behaviour to refine game mechanics, identifying issues like the difficulty of game levels, bugs, and usability issues.

- Monetisation and marketing: Collected data is used to support targeted marketing campaigns, allowing different actors in the ecosystem to determine optimal timings, content, and audience for advertising.

- Personalisation and customisation: Another common purpose is game personalisation. Data is used to automatically customize content and services, tailoring game rules and content to suit the player's skill level, gameplay preferences, or playing style. This purpose implies very often different types of profiling.

- Fraud prevention and safety: Telemetry data may enable the detection of cheating behaviours to maintain the integrity of the game, to prevent fraud and enforce the terms of service.

2.3 Behavioural inference

Personal data processing within video games enables the generation of new information derived from analysing the one directly collected from the user (mainly during the account creation and management processes but also relying on feedback gathered using in-game polls and surveys) and passively collected raw data (telemetry) generated during gameplay.

As already discussed, telemetry can log raw hardware and device inputs (such as webcam and multi-modal sensor inputs, mouse clicks, keystrokes, button press timings, stick drifts, trigger pressures, device tilt, and vibration responses). In addition, movement vectors, deaths, quest completions, item interactions, and session durations are recorded with precise timestamps. Advanced telemetry may include heatmaps that track gaze or cursor paths, or progression trees that map decision branches. Combining this information with other information, for example, related to account creation and management (chat logs, emote usage, friend lists, and group formations, etc.) or even from external sources, inferences can be produced.

Inference production is the process of mining collected data for patterns and statistical relationships to derive additional personal information that the user did not explicitly or implicitly provide. This process involves applying advanced data analysis methods, often relying on machine learning or Artificial Intelligence. Raw streams feed feature engineering, then CNNs[3] analyse voice pitch, volume, and speech disfluencies for arousal or frustration; NLP solutions[4] and graph algorithms classify social roles (leader, troll); unsupervised clustering (K-means/DBSCAN[5]) groups playstyles; supervised

[3] Convolutional Neural Networks (CNNs) are deep learning networks designed for processing structured grid data (such as images or time-series telemetry streams) and learning hierarchical features via filter (or kernel) optimisation.

[4] Natural Language Processing solutions (NLP) are focused on enabling machines to understand, interpret, and generate human language.

[5] K-means and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) are unsupervised clustering machine learning algorithms used to group data points based on similarity (and identify outliers as noise).

models (XGBoost[6], LSTMs[7]) predict churn/emotion from time-series; reinforcement learning adapts NPCs based on inferred archetypes like “achiever” or “socialiser”, real-time edge processing enables dynamic difficulty or content generation, etc.

Players are, again, frequently unaware of the nature and amount of their data collected and processed. Table 4 provides a non-exhaustive overview of said data.

Data type	Specific data elements	
Skills and abilities	Inferred levels of competence in:	
	■ Strategic thinking	■ Math fluency
	■ Quick reflexes	■ Teamwork ability
	■ Aiming accuracy	■ Memory retention
	■ Multitasking	
Emotions	Inferences to detect:	
	■ Stress/distress	■ Confidence
	■ Fun	■ Disappointment
	■ Frustration	■ Valence of emotions (positive/negative reaction to stimuli)
Personality traits	Inferences to assess:	
	■ Aggressiveness	■ Untrustworthiness
	■ Risk aversion	■ Tenacity and determination
	■ Goal orientation	■ Overall psychological maturity

[6] Extreme Gradient Boosting (XGBoost) is an optimised open-source library designed for efficient and scalable gradient-boosted decision trees (GBDT) widely used for classification, regression, and ranking.

[7] Long Short-Term Memory networks (LSTMs) are a specialised type of Recurrent Neural Network (RNN) designed to learn long-term dependencies in sequential data by overcoming the vanishing gradient problem and model temporal patterns.

Data type	Specific data elements
Financial status and consumption habits	Inferences to determine if a player is: ■ Frugal, fiscally responsible ■ Impulsive ■ Wasteful ■ Eager to test new products or services
Other inferences	Age and gender Body measures and biometric information Cultural background Physical and mental health condition Substance and drugs use Cognitive processes

Table 4. Personal data processed for behavioural inference

The processing of this data may serve different purposes:

- Game enhancement and technical improvement: Profiling helps to analyse the difficulty of game levels, adjust game mechanics, and address usability issues.
- Monetisation and marketing: Profiles are created to predict purchasing behaviour, identify financially exceptional users (sometimes referred to as "whales", players spending an unusual large amount of money on in-game purchases), and support targeted or precision marketing campaigns. Different actors in the ecosystem can create psychological profiles based on gameplay used, for example, to make players spend more time or purchase premium content. Again, this purpose often involves profiling.
- Personalisation and customisation: Inferences are used to automatically customize content and services to suit the player's skill level, gameplay preferences, or playing style.
- Fraud prevention and safety: Inferences may enable the detection of harmful behaviours, content moderation, etc.

3. Data protection threats and risks

Personal data processing in video games poses specific threats and risks beyond traditional IT environments, driven by pervasive telemetry, behavioural profiling, and increasingly sophisticated monetisation models. This section identifies the main data protection threats in the video game ecosystem following the LIINE4DU methodology[8], and analyses their potential impact on rights and freedoms of data subjects, as a basis for providing recommendations and good practices later in this document.

[8] An introduction to LIINE4DU 1.0: A new privacy&data protection threat modelling framework, https://www.aepd.es/guides/technical-note-introduction-to-liine4du-1-0.pdf

3.1 Linkability

This threat involves associating different data items or data subject's actions to learn more about the data subject or their group. Players can be linked to their transactions and activities through different pseudo-identifiers explicitly or implicitly collected.

Online game publishers and storefronts may use technologies such as cookies, web beacons, tags, or device/browser fingerprinting to track individual users and their activities across different game sessions, even when they are not logged in.

Cross-game tracking is often possible simply from a player's nickname, which can be the same across different games and platforms. Another way of tracking is based on using a data subject's unique characteristics, such as how they handle interfaces (keyboard, mouse, controller, etc.) or their individual playing style (e.g., a specific course of action in strategy games or a driving profile in racing games).

Furthermore, players' data is rarely confined to the game publisher's or storefront's internal servers. It is frequently combined with external data sources. These actors often share user data with various third parties, including gaming networks, data brokers, middleware and analytics providers, and advertising platforms. Shared information may then be matched with third-party data about the same user.

It must be considered that games often prompt users to link their social media accounts, further increasing the risk of linkability threats being materialised. Additionally, playing games on external devices, such as smartphones, introduces additional ways to collect data and combine game information with third-party datasets.

The extensive collection of linkable data can feed advanced profiling methods, often based on Artificial Intelligence, linking raw data to sensitive personal traits: skills and abilities, emotions, financial status, vulnerability to addictive design, etc., used by different parties to predict and influence future users' behaviour. This may lead to exploitation and manipulation (from increasing the manipulative effect of targeted advertising to swaying political opinions or making players spend more time in the game and feeding or encouraging addictive tendencies). Linking can be used to profile users as "susceptible to spend" or "whales", targeted to be induced to spend exorbitant sums of real money within the game.

Discrimination inside and outside the video game ecosystem (given data sharing practices) can also be an impact. For example, linkable data and inferences may be used to compute a "financial risk factor" from gameplay behaviour, potentially leading to a user being denied a loan or a credit line extension. Similar inferences could also be used to assess a player's essential qualities to determine their suitability for certain jobs.

3.2 Identification and doxing

Identification involves one of the actors of the video game ecosystem learning the identity of a data subject directly (for example through the processing of identifiable information or leaks) or indirectly (for example through deduction or inference).

Registering with ecosystem actors to access the latest games and features usually requires providing real-world identity data. This makes the threat materialise almost immediately, as registration

data typically includes personally identifiable information such as full name, email address, postal address, and credit card details.

This is exacerbated by the linking threat, because in many cases, only one actor in the ecosystem knows the player's identity, but through linking and profiling, others may end up knowing it as well. Even when a player does not reveal their real identity, integration with social network accounts or the use of smartphones may reveal it. Additionally, by customizing characters and profiles (such as through nickname, age, language, or gender) players may unintentionally disclose aspects of themselves, contributing to identification. Furthermore, modern gaming devices frequently collect biometric data (voice, facial features, movements, body size, and eye patterns) which on their own could be enough to enable player identification.

The identification threat is often combined with inferred behavioural and psychological traits. As a result, the gaming ecosystem can be a powerful tool for digital surveillance, making players susceptible to external exploitation and unexpected misuse of their data.

Doxing is essentially the public release of private information about an individual (such as their real name, home address, or employment details), which the individual typically intended to keep confidential. When the real-world identity of a player is publicly released, whether through intentional malice (harassment by a peer) or a data breach, the identification threat is realised as a doxing event. Female players, in particular, may face risks of harassment and often adopt strategies such as hiding their gender by carefully managing their game profile/character or avoiding voice chats to steer away harassers. If precise identifying information including location data is publicly released, the doxing consequences extend beyond the digital realm and can compromise their physical safety.

3.3 Inaccuracy

Inaccuracy threats in video games arise when personal data (including raw data and inference-based data) is incomplete, obsolete, or wrong with regard to the purpose of the processing.

If a player's data, including login attempts and security-related aspects, is not continuously kept up to date, it may become obsolete and affect account management and security. More specifically, games frequently specify age limits (e.g., +13 or +18) and rely on age proof provided upon sign-up. If the age assurance process is not reliable and not sufficiently robust, and an obsolete or incorrect age profile is used, this may prevent adults' legitimate access or allow non-permitted children access, with consequent safety implications. Telemetry data is often used to customise game content and services according to individual playing styles and preferences. If this data is inaccurate, personalised experiences may become irrelevant or mismatched, negatively affecting the gameplay experience and thus reducing player satisfaction.

Telemetry data is also essential for maintaining the integrity of online games, particularly for detecting cheating. If telemetry data used for detection is inaccurate or misinterpreted, a legitimate player could be incorrectly flagged for dishonest behaviour, potentially leading to unfair consequences such as suspension or a ban. Additionally, if flaws in the system prevent the accurate detection of cheats, genuine cheaters will be able to continue cheating. This then grants unfair advantages and compromises the gaming experience for honest players. Furthermore, cheaters who use bots or hacks can increase the supply of virtual goods, thereby deflating the value of the commodities earned by legitimate players, leading to a loss of profit for those players in particular, and a distortion of in-game economies in general.

As mentioned before, gaming companies use advanced data analysis methods to mine gameplay data for patterns and statistical relationships, generating derived personal information that the user did not explicitly provide. If the raw data is noisy, incomplete, or corrupted (e.g., due to connectivity issues, server lag, or software bugs) or the inference mechanisms have flaws, the derived behavioural inferences will be inaccurate but may still be used for automated decision-making. For example, an automated stealth assessment conducted within the game environment tries to measure competence across skills such as strategic thinking, fine motor skills, or memory retention. If the underlying raw data is flawed, the assessment of the player's abilities might be inaccurate, potentially misclassifying their competencies, knowledge gaps or learning difficulties, consequently impacting their game experience in a negative way.

As mentioned before, gameplay data can be analysed to compute a "financial risk factor", which may then be shared with third parties, such as insurers or employers. If the underlying telemetry data (which can indicate if a user is frugal, fiscally responsible, or wasteful) or the outcome of the inference systems are inaccurate, a player could face discrimination in the real world, such as being unfairly denied a loan or a job, based on a faulty assessment derived from their virtual activities.

Inaccuracies can also materialise in the information shared with other users or the public, impacting the player's social experience and reputation. Social features enable other players to see a player's username, avatar, and game progress, as well as gameplay-related information such as high scores. If the underlying progress data is inaccurate (e.g., due to cheating that goes undetected or game bugs affecting metrics), the representation of the player to their peers will be wrong, potentially affecting their social standing or the fairness of matchmaking.

3.4 Non-repudiation

Player actions and game activity are persistently tracked, logged, and retained. This recordkeeping lays a foundation for non-repudiation threats: a data subject cannot deny involvement in actions, such as communicating with other players, being suspected of cheating, or making a financial transaction:

- Online games, particularly those with multiplayer modes, routinely record and store player-to-player communications (such as chat text and voice data). This monitoring aims to protect users by identifying discussions, offensive language, and abusive interactions.

- Gameplay monitoring (telemetry) continuously records player behaviour, performance, actions, and decisions. Analysing this high-granularity data can uncover cheating and other unfair practices, attribute these behaviours to specific players, and enforce fair play.

- When real money is exchanged for in-game content, absolute record-keeping is necessary to establish liability and prevent financial fraud.

Together, these mechanisms create a strong chain of evidence that allows the ecosystem to definitively show who performed which actions. In some cases, such evidence is a legal requirement or essential for safety and core functionalities. However, these systems also eliminate the player's ability to plausibly deny any action, whether positive (such as completing challenges or game levels) or negative (such as playing highly violent video games very frequently, harassment or cheating), even when it is not legally mandated to keep a record or when it is not strictly necessary for providing the core service. The main impact of non-repudiation mechanisms is a lack of plausible deniability, which may lead to social and legal consequences inside and outside the game environment.

If a player is found to have violated terms (abuse, fraud), for example, the records justifying the decision to enforce a penalty such as a permanent ban may be retained indefinitely. These records may prevent the player from creating a new, non-sanctioned account in the same game or platform, or in a different one, now or in the future. Moving outside the gaming ecosystem, an employee could be fired because the granular telemetry logs detailing their time spent playing are shared with their employer, thereby providing irrefutable, time-stamped evidence used in a formal employment termination: the employee was playing during their work hours and cannot deny it.

Furthermore, because non-repudiation often relies on complex, proprietary algorithms, players who wish to challenge an automated decision (e.g., an incorrect cheating penalty) could face significant difficulty trying to do so. The system holds the evidence of the action, even if the player argues the action was unintentional or misidentified by the algorithm. The potential impact of a combination with an inaccuracy threat or an unintervenability threat (to oppose being the subject of an automated decision) should be considered here.

3.5 Data breach

Data breaches pose a critical threat to the video game ecosystem, as major incidents have exposed significant amounts of player information collected and processed by game companies in the past. With the number of online gamers surpassing 1.3 billion worldwide in 2025, the potential scope of these breaches is vast.

A data breach involves unauthorised security access leading to accidental or unlawful destruction, loss, alteration, disclosure of, or access to personal data. Players' personal data, such as names, passwords, email addresses, phone numbers, and even financial data, may be compromised. This information can be sold or used to launch further attacks, greatly increasing the risk of identity theft or fraud and leading to broader consequences, such as illegal purchases or loans made with the stolen data.

Credential exposure in data breaches often drives account takeovers, resulting, for example, in the loss of in-game assets and currency. When players reuse passwords across accounts, a single breach enables adversaries to access multiple gaming or even more sensitive accounts, a scenario known as credential stuffing.

Since the industry also processes vast amounts of telemetry and inferences from behavioural data, unauthorised disclosure could expose intimate insights into a user's skills, emotions, and personality traits, as well as their in-game communication, cheating flags, and other sensitive information.

3.6 Deception

Dark patterns, also known as deceptive designs, threaten players by using manipulative user interfaces, primarily motivated by monetisation. These designs influence player behaviour, often leading to unintended disclosure of personal data or financial loss by increasing the likelihood that players will share personal data or spend money.

Deceptive design patterns use specific manipulative techniques to trick players into decisions they would otherwise avoid. These techniques exploit psychological vulnerabilities and cognitive biases by intentionally varying emotion, colour, language, options, etc.

For example, some games make signing up with social media accounts easier than signing up with an email address. Other games offer in-game rewards to encourage players to link to their social media accounts or share contact lists. Dark patterns can also pressure players into subscribing or clicking ads. Often, a game claims that cancelling before a free trial ends is easy, when it is actually difficult. Other patterns encourage microtransactions, loot boxes, or pay-to-win mechanisms, thereby increasing the pressure to spend money during gameplay.

In general, deceptive patterns are used to actively encourage and reward players for activities that may have negative impacts on them, but they often receive no clear information about these negative consequences of their decisions, which may also be heavily "guided", "nudged", or "influenced".

Addictive patterns form a subset of dark patterns. They are design practices intended to encourage users to spend much more time on digital platforms, or to engage more deeply than is healthy or expected. The main risk with addictive design is excessive, compulsive use of digital products, such as video games. Negative consequences include time loss (users spend far more time than planned) and psychological harm (potentially contributing to mental health issues). Notably, "gaming disorder" is recognised as a medical condition in the WHO's International Classification of Diseases (ICD-11), effective since 2022.

Addictive patterns such as playing by appointment, grinding and mere exposure, periodic rewards, or social pressure and comparison are frequently used in video game design. Because actors participating in the ecosystem possess massive amounts of information about players, this informational asymmetry can be used to manipulate their behaviour, making it difficult for users to understand how they are being influenced and to protect themselves. When a player invests more time in a game, the game ecosystem collects a greater volume and variety of high-dimensional behavioural data. The longer the playtime and the larger the collected dataset, the easier it becomes for developers and platforms to apply advanced data analysis methods to uncover patterns and infer sensitive personal information that the user never explicitly provided. This process transforms raw data into deep, actionable knowledge about the player. This acquired knowledge informs the precise deployment of deceptive and addictive design patterns to maximise data sharing, revenue generation, engagement, and commitment.

3.7 Data disclosure

The data disclosure threat in video games involves collecting, storing, processing, or sharing/transferring personal data beyond what players anticipate, expect, or consent to.

Modern online games can collect enormous quantities of high-dimensional, highly granular user data, often exceeding what is necessary for core gameplay. The previous section introduced the types of personal data that games usually process, including registration and account management, gameplay monitoring, and behavioural inference. This section has also discussed, with respect to other threats, the capability to infer sensitive personal data, such as financial risk scores.

A key distinction in data disclosure threats must be made between data explicitly provided by players and data collected or inferred implicitly (through telemetry or behavioural analysis). These categories differ in users' awareness and the types of information revealed.

Explicitly provided data includes information users enter themselves (name, email, age, gender, phone number, bank details) during registration or transactions. Players know they are sharing this and may adapt their behaviour accordingly. For example, they might protect themselves by using

fake profiles. In contrast, telemetry and inferred data are collected automatically from in-game actions, device usage, or sensors, often without the user's awareness. Games analyse this raw data to infer sensitive information that users have not intentionally provided. Since players typically do not realise the extent of such data collection or the inferences drawn from it, they have little control over the sensitive information disclosed.

Implicit data collection greatly expands the range of information exposed. As mentioned, data from gameplay and sensors can reveal far more than demographical information alone. For example, emotions, skills, interests, habits, personality traits, socioeconomic status, and aspects of physical or mental health can also be revealed. Collection methods such as client-side anti-cheat software or integrated sensors (cameras, microphones, eye-tracking) can intrusively access a user's device or even their body.

It must be considered that gaming devices increasingly use sensors to collect highly sensitive data, such as voice, gestures, and facial expressions. AR/VR headsets, for example, capture biometric data including posture, eye movements, skin conductance, and heart rate, enabling the inference of highly sensitive information.

Non-invasive EEG (electroencephalogram) headsets are now being introduced into the video game ecosystem, often referred to as Brain-Computer Interfaces (BCIs). These devices measure electrical activity in the brain using scalp sensors. Software then filters out noise and applies machine learning or AI models to map particular brainwave patterns or mental states (such as "focus" or "relaxation") to in-game commands, like moving, jumping, or triggering an ability. There are two main paradigms in use. The first, called "active" or "mental command" BCIs, requires players to train the system to associate a specific imagined action or mental strategy with a discrete game command (for example, thinking "push" to move an object). The second, termed "passive" or neuroadaptive systems, continuously monitors cognitive or emotional states (such as engagement, stress, or fatigue) to adapt the game's difficulty, pacing, or content without requiring the player to issue deliberate mental commands. Neurogaming constantly collects and processes neurodata, which can reveal information about players' mental states, emotions, and other sensitive traits.

Modern sensors can also monitor a user's position and surroundings, sometimes even capturing data about bystanders. Games may also request access to data from other apps on the same device or from a user's social media, such as contacts, documents, emails, and files. Data disclosure threats often culminate in the broad distribution of player information to third parties, affiliates, or other players. Game companies regularly share player data with parties such as advertisers, partners, gaming networks, middleware providers, analytics providers, and aggregators. As games operate globally, data may be transferred to countries with less robust data protection laws than those of the player's country.

3.8 Unawareness and unintervenability

This threat involves insufficiently demonstrating compliance or insufficiently informing, involving, or empowering data subjects in the processing of their personal data.

Video games are complex digital services that very often use advanced inference, profiling, and even surveillance mechanisms. These features may be deeply integrated into the game environment, operating in ways that are either not visible or obvious to players.

Games collect a massive amount of detailed user data, which ordinary players cannot easily trace. Players are often unaware of both the type and quantity of data gathered, as well as how it will be used. Advanced data analysis techniques draw personal inferences from hidden patterns in gameplay or sensor data, making these activities hard for users to anticipate. Furthermore, many players do not realise that in-game communications (such as voice chats) might be monitored, recorded, or shared with third parties. The immersive, fictional nature of video games can distract players from very real privacy risks, creating a false sense of anonymity, potentially encouraging more revealing behaviour.

Even though regulations require a high level of transparency, most games rely mainly on privacy policies as their primary means of informing players. These documents tend to be lengthy, dense, and filled with legal jargon, often making them hard to understand. As a result, many users skip reading them and start playing right away. The policies often use vague wordings, such as "improving user experience" as a purpose for behavioural inference processing activities, "support advertising services" as a purpose for profiling and sharing player data with third parties, or "deliver personalised features" to describe how data is collected and used. This lack of detail fails to explain the legal basis for processing personal data in the first place.

The unintervenability threat arises when players, even if made aware of the risks, lack simple, effective ways to control their data. This makes active intervention or decision-making about their privacy difficult or impossible.

For example, many games do not provide accessible or meaningful controls for managing personal data, contrary to player expectations. Even when privacy settings exist, they are rarely centralised and often difficult to interpret, leaving players confused about their options and sometimes effectively compelled to agree to privacy-invasive setting (such as enabling tracking) to access full game features.

Players should be able to exercise their rights, for example to easily access, correct, and delete their data. However, overly complex or lengthy privacy settings or policies make it difficult to manage personal data. Additionally, withdrawing consent should be as simple as giving it in the first place.

3.9 Threats to children and other vulnerable players

The video games ecosystem poses heightened threats to children and other vulnerable players due to a combination of their developmental stage, high engagement level, limited digital literacy, and the industry's focus on their data collection and monetisation. While all players face the same risks, children and other vulnerable groups are usually less equipped to recognise or mitigate their impact and more susceptible to manipulation.

Children, as a vulnerable class of data subjects, require enhanced protection online due to limited awareness of data processing risks, particularly in digital settings such as video games. The GDPR mandates that companies reasonably verify parental or guardian authorisation when processing minors' data on the basis of consent, especially for those under 16 (or a lower age, as set by individual Member States).

Children and teenagers constitute a significant portion of players and are frequently targeted by marketing. They may be predisposed to exchange personal data for incentives. Often, children lack awareness of privacy settings and seldom take online privacy precautions. Many do not recognise what data is collected or the purposes for which it is processed.

Children may be misled or exploited by online marketers using special techniques and dynamic ads tailored to their profiles and behavioural patterns. Data collection, which often occurs through implicit mechanisms, can result in children being treated as algorithmic assemblages. This may limit their complexities, potential, and opportunities. The resulting risks include identity theft, loss of reputation, and both current and future discrimination, even stigmatisation.

Online interactions may expose vulnerable players to harassment, discrimination, and bullying if personal identity attributes are shared. Disclosure of race, gender, sexual orientation, or political ideas can result in abuse. Gaming environments often mirror societal hostilities, with minorities facing inappropriate behaviours. Age, religion, nationality, or gaming skills can also make individuals targets. Children, who are still developing social skills, are especially at risk and require extra protection. Malicious actors further exploit in-game communication tools, like voice and text chats, to spread hateful, extremist narratives and disinformation, affecting thousands, including minors. There are risks of exploitation, such as cheating to gather rewards or steal virtual assets. Impersonation is also a concern, such as when a player pretends to be an authority to gather sensitive data. These risks can lead to serious consequences beyond gaming, including identity fraud and geolocation issues that may affect safety and physical integrity.

The rise of free-to-play (F2P) models and microtransactions exposes children to marketing pressures they may not be equipped to handle. Concerns around monetisation include the possibility of gaming taking over daily life (addictive behaviours) and the risk of overpaying. Children, especially young ones, may be less resilient to marketing pressure or less savvy about the value of products, particularly when platforms allow for quick, simple purchasing of in-game items. Deceptive design can exploit vulnerabilities by creating the impression that gamers who do not make in-game purchases will lose out on exclusive content or gameplay advantages. This social risk of falling behind peers who are spending money can encourage impulsive buying or gambling addiction. The same happens with time-limited or one-time-only offers targeted at children. Furthermore, randomised rewards, such as loot boxes, pose specific risks to these vulnerable players.

The following sections provide actionable recommendations and good practices to assist controllers and processors in the video games ecosystem with complying with core GDPR obligations, including the principles of Article 5 (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability), legal bases and special conditions under Articles 6, 8 and 9, data subject rights (including safeguards against solely automated decisions under Article 22), data protection by design and by default (Article 25), and security of processing (Article 32). The recommendations provided help to avoid or mitigate threats such as those identified in section 3. They are not a summary of well-known generic recommendations to comply with GDPR data protection principles and obligations, but rather specific recommendations regarding specific aspects present in video games.

While these specific measures offer a practical compliance path tailored to each lifecycle stage and processing activity, actors remain free to identify and implement alternative approaches that equally satisfy these requirements. Any deviations should be documented with clear justification demonstrating equivalent protection levels, and full accountability for the chosen design or implementation should be ensured.

4. Recommendations and good practices during Pre-production and production

Pre-production is the stage at which a video game's conceptual, narrative, and technical identity begins to form. It is also the phase in which the controller's long-term compliance posture is determined. By the time a game reaches launch, many of the consequential GDPR decisions – such as the necessity and proportionality of particular data processing activities, the purposes that can legitimately be pursued, the categories of personal data collected, and the architecture of data protection by design – are already embedded in the game's structure. For this reason, the GDPR's core principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation and data protection by design and by default, must inform early creative and technical decisions rather than operate as constraints appended late in the development cycle. Compliance is not only compatible with innovative game design but can also improve clarity, predictability, and player trust throughout the game's entire lifecycle.

4.1 Identifying GDPR roles and responsibilities

The different actors participating in the video games ecosystem need to determine their role under the GDPR (controller, joint controller or processor) to understand their legal obligations and liabilities concerning personal data processing activities[9]. A single entity might play different roles depending on the specific processing activity. Remember that once established as a controller, you bear primary responsibility under the GDPR for ensuring lawful, fair, and transparent processing, including implementing appropriate technical and organisational measures, cooperating with data protection authorities, and being accountable for all downstream processing, including that carried out by processors such as cloud or ad tech providers. Your key obligations include, among others, identifying a lawful basis for each processing activity, providing clear and accessible privacy information to players, respecting data subject rights, and maintaining records of processing and data breaches. Game ecosystem controllers must also conduct Data Protection Impact Assessments when processing is high risk (for example, profiling, behavioural advertising, or processing children's data), put in place binding contracts with processors, and demonstrate data protection by design and by default throughout the game's lifecycle, from account creation to post production and live service operations. A single entity might play different roles depending on the specific processing activity. Regardless of your industry role, you must answer these three fundamental questions for each specific processing activity (account creation and management, telemetry, behavioural inference) conducted through the game lifecycle:

1. Who decided to conduct the processing activity?

2. Who defined the purpose (the "why") and the essential means (the "how", such as data types and retention periods) of the processing?

3. Who is processing data based on the documented instructions of another?

[9] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

For all actors, a good practice is to require that each new game or feature pass through a "GDPR role gate" at the end of the pre production and production stage:

- **Step 1:** List personal data processing activities, at least, under these three headings: account creation and management, telemetry, and behavioural inference. Consider that, during this video game lifecycle stage, personal data of members of internal teams (development, QA, lab and research) will be processed. But also, of members of a "close circle": external testers (screened playtest participants, invited community members), sign-ups and early access players, etc. We will refer to all of them as "early access players" in this section, and they may or may not have employment contracts with any of the actors in the ecosystem. In later lifecycle stages, it will primarily be the personal data of players that will be processed.

- **Step 2:** For each data processing activity, answer the guidance questions below and mark: controller/joint controller/processor.

- **Step 3:** Ensure that Joint Controllership Agreements (Article 26 GDPR) or Data Processing Agreements (Article 28 GDPR) are signed whenever these relationships exist. Guarantee privacy notices, procedures, DPIAs, etc. matching the identified roles. All these measures must be implemented before release.

Document your results; you need to be able to explain why you chose a specific GDPR role in each case. Additionally, reassess regularly as video games and their ecosystems evolve (e.g., the addition of cross-platform identities, AI-based personalisation, or changes to telemetry).

In this specific stage of the video game lifecycle, you can follow the following per-role recommendations, do it always on a case-by-case basis, per data processing activity.

4.1.1 Hardware suppliers

Guidance questions:

- Do you define the purposes of the hardware platform account (access control, cloud saves, cross-device identity, anti-cheat, marketing)? If yes, you are a controller for that account.

- Does any developer or publisher co-decide what data must be in the early access player account and how it is used, for example for testing or feedback? If yes, consider joint controllers.

- Are you simply providing a login SDK (no access to underlying identifiers, no reuse for your own purposes), under written instructions? If yes, you are a processor.

- Are you defining what platform telemetry is collected (session length, device usage, error logs) or inferences made, and reusing them for your own analytics and product decisions? If yes, controller.

- Are you exposing telemetry APIs to publishers so both of you decide metrics used to test the game? If yes, potential joint controllership, especially where you jointly design dashboards and KPIs.

In summary, per data processing activity type:

- Account creation and management (hardware platform account): likely controller, sometimes joint controller or processor.
- Gameplay monitoring (platform telemetry): controller, joint controller when telemetry is co-used with publishers.
- Behavioural inference (platform-level inferences): likely controller.

4.1.2 Creators, designers and developers

Guidance questions:

- Are you issuing game accounts to testers or staff under your own terms and privacy notice? If yes, you are controller for those accounts.
- Do you decide to keep account credentials or IDs after the contract to reuse them in other titles? If yes, separate controller role for that reuse.
- Are you creating or managing early access player accounts fully under a publisher's documented instructions and platform rules? If yes, processor for that processing.
- Who decides which telemetry events are instrumented (e.g., level completion, button presses, chat events) and why? If you decide or co-decide beyond technical necessity, you may be controller or joint controller.
- Will you store telemetry in your own environment and reuse it across titles to improve design, balancing or AI models? If yes, separate controller.
- Are you contractually obliged to collect and forward raw telemetry exactly as specified by publisher, with no independent reuse? If yes, processor.
- Are you training models on test or live data to understand playing styles and inform future titles beyond the commissioning project? If yes, controller for that profiling.
- Are you only implementing models specified by the publisher, deployed on their infrastructure, without reusing data or outputs? If yes, processor.

In summary, per data processing activity type:

- Account creation and management (game accounts): controller for own test accounts; processor if accounts are managed for a publisher.
- Gameplay monitoring (game telemetry): processor when collecting telemetry solely for the publisher, controller when using data for own R&D across projects.
- Behavioural inference (game-level inferences): controller when building models for own purposes, processor when building models solely for publisher under instructions.

4.1.3 Development technology providers

Guidance questions:

- Are you using own service account data (email, handle, usage) to manage licences, support, and improve your tools? If yes, controller of that processing.
- Do you expose a white-label login where all account decisions (fields, retention, reuse) are set by the client, and you cannot repurpose data? If yes, processor.
- Does your service send player/device data to your own servers by default (e.g., crash info, performance counters) for your product improvement? If yes, controller of that telemetry.
- Can creators, designers and developers disable or heavily configure data capture, or is it "baked in"? In cases where there is less configurability and where there is the possibility for you to reuse, more clearly controller.
- Do you only process telemetry in the customer's environment with no access or reuse? If yes, you may identify as processor but recognise that mere local library code with no access may take you out of GDPR's "controller/processor" dichotomy for that specific data processing.
- Are you offering generic "engagement optimisation" or "personalised offers" modules that all games can plug into, and do you tune them using cross-game data? If yes, you are controller of that profiling engine, even if studios are also controllers for their use.
- Are you jointly defining segmentation logic with studios for specific campaigns? If yes, consider joint controllership.
- If you only host and compute models with no independent reuse or decisions, and studios fully define the logic, you may be processor.

In summary, per data processing activity type:

- Account creation and management (own service accounts): controller, processor if purely authenticating for a client.
- Gameplay monitoring (service telemetry): often controller, sometimes joint controller; may be processor if truly instruction bound.
- Behavioural inference (service-level inferences): controller for generic behavioural models (possible joint controller), sometimes processor.

4.1.4 Publishers

Guidance questions:

- Do you decide to create publisher-wide IDs that link the player across different games, platforms, and telemetry? If yes, controller for that identity graph.
- Does a platform (hardware supplier/console or storefront) co-decide how your accounts link with theirs and for what joint features? If yes, joint controllers.

- Are you operating accounts only as a service for another brand under its logo and policies? If yes, processor for that processing.
- Do you design the telemetry strategy for this video game lifecycle stage (what to measure, for how long, and for what decisions)? If yes, controller.
- Are you combining telemetry from several hardware platforms or storefronts to build unified early access player profiles? If yes, controller role.
- Do contracts with studios or development technology providers accurately reflect their role? If you give detailed instructions and forbid reuse, they should be processors for your telemetry.
- Are you using behavioural inferences to test or improve the game at this stage? If yes, controller for profiling.

In summary, per data processing activity type:

- Account creation and management (publisher accounts): controller, sometimes joint controller with creators, designer and developers.
- Gameplay monitoring (publisher telemetry): controller for telemetry, joint controller with other actors where they co-decide.
- Behavioural inferences (publisher-level inferences): controller for gameplay-based profiling, sometimes joint controller with hardware suppliers/development technology providers/ storefronts.

Note:

Special mention goes to mods. Mods are user-made changes to a video game's assets, code, rules, visuals, or features. A developer makes a game more "moddable" by providing tools, open file formats, or scripting support. Games with strong mod support often keep communities active because mods extend replay value and creativity and can even reshape the game's identity. Mods can replace textures, change character models, add items, tweak balance, or adjust difficulty. More advanced mods inject scripts or connect to the game's logic to add mechanics, UI, or create total conversions that feel like new games built on the original engine.

Mods can reshape data flows inside a game. They can change who collects data, what data is collected, and who is responsible for it under the GDPR. A mod may add online features, connect to external servers, log gameplay behaviour, or integrate SDKs. These SDKs may process identifiers, IP addresses, device data, or voice/video content. That means the legal question is not only "is the mod allowed?" but also "who is the controller, who is the processor, and what lawful basis applies?" In practice, the mod ecosystem can create completely new risks. This affects game publishers, mod platforms, server operators, and mod creators, especially when mods use telemetry, accounts, chat, voice, analytics, anti-cheat, or third-party services.

If the publisher simply provides a modding toolkit but does not decide the mod's data processing, the modder or the mod service may bear primary responsibility for its own processing. But if the publisher promotes, preinstalls, curates, or technically enables the mod's data collection, the publisher can still have GDPR duties and may be subject to joint-controller analysis.

4.1.5 Storefronts

Guidance questions:

- Do you reuse account data for cross-game purchase history, recommendations, and social features you define? If yes, controller.
- Do you and a specific publisher co-design a loyalty or progression system that needs shared accounts? If yes, joint controllers for that scheme.
- Are you collecting launcher-level telemetry (time in launcher, clicks, searches, time in each title) for your own UX, recommendations, and A/B tests? If yes, controller.
- Do you allow publishers to embed their own telemetry tags, but you do not decide purposes/means, nor reuse the data? If yes, they are likely independent controllers, and you supply infrastructure.
- Do you jointly design analytics programs (e.g., cross-promotion experiments where you and the publisher pick segments and metrics)? If yes, assess joint controllership.
- Are you profiling early access players' store and game behaviour to recommend titles, promote specific events, or personalise offers? If yes, controller.
- Do you run joint marketing campaigns where you and a publisher co-decide targeting criterion? If yes, check whether this is joint controllership. At minimum, both are controllers exchanging profiles.

In summary, per data processing activity type:

- Account creation and management (storefront account): controller, potentially joint controller with publishers for co-branded programs.
- Gameplay monitoring (storefront telemetry): controller for telemetry used to run and optimise the store/launcher, joint controller if co-deciding on telemetry with publishers.
- Behavioural inference (storefront-level inferences): controller for own recommendation and ad-targeting systems, sometimes joint controller with publishers for joint campaigns.

4.2 Identifying personal data processing activities, purposes and lawful bases

4.2.1 Creating a detailed inventory of personal data processing activities

Before progressing to the release stage, data controllers must produce a comprehensive inventory or record describing all categories of personal data they will process at all stages of the video game lifecycle, not just in this first one. This includes obvious identifiers such as usernames, email addresses, and IP addresses, as well as the more subtle categories common in gaming, such as telemetry and behavioural inference. In addition, a description of the categories of data subjects, the categories

of recipients (and, where applicable, transfers of personal data to a third country or an international organisation), and retention periods.

It is essential to separately identify special categories of personal data, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation (Article 9 GDPR). All actors must explicitly prohibit the collection of special categories by default, for example, using interface rules to ban open "bio" fields and designing filters to anonymise chat content or behavioural tags that might reveal sensitive insights.

During the pre-production and production stage of a video game, which encompasses everything from initial pitching to final pre-launch preparations, all ecosystem actors must adopt a proactive approach toward data protection to meet the requirements of Article 5 GDPR. Each data category must be clearly linked to a specific, explicit, and legitimate purpose. Generic formulations such as "improving the game" or "enhancing player experience" do not satisfy Article 5(1)(b). Instead, purpose descriptions should reflect the actual use cases as transparently and as detailed as possible, such as "detecting bugs", "balancing difficulty", "refining matchmaking", or "identifying cheating". To uphold the principles of lawfulness, fairness, and transparency, all actors should start by defining strict data schemas for account creation and removing "nice to have" fields that do not directly support the defined purposes. This means specifying exact attributes for developer, SDK, tester, or player accounts, and prohibiting arbitrary tags or free-text fields that could inadvertently embed personal data of data subjects.

Purpose limitation and data minimisation are further achieved when actors justify every telemetry event or inference against specific purposes, such as "technical necessity" or "analytics" in their design specs. Controller should follow the evolution of the hardware, operating systems and development technology and their functionalities, in particular in terms of minimisation of the processed data (for example, collection of identifiers, network addresses or geolocation).

Crucially, storage limitation should be codified early; actors should document retention periods (e.g., deleting playtest accounts or raw telemetry logs 30 to 90 days after a test phase) and implement these rules via automated purging or scripts in the release pipeline.

Accountability is reinforced when these decisions are recorded in project checklists or data dictionaries. All this information is also essential for drafting accurate privacy notices, designing consent flows and identifying high-risk processing activities that require a DPIA under Article 35.

4.2.2 Documenting legal bases for each purpose

After mapping the purposes of each data processing activity, each must be paired with a legal basis under Article 6. The specific nature of processing activities and the variety of purposes pursued usually require using different legal bases for different processing activities, combining such legal bases as:

- Consent (Article 6(1)(a)), for example, for optional personalisation, behavioural advertising, cross-platform profiling, and any processing going beyond reasonable user expectations.

- Processing is necessary for the performance of a contract (Article 6(1)(b)), for example, for essential gameplay functions and account creation.

- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (Article 6(1)(f)), for example, for proportionate security or stability analytics, subject to a rigorous balancing test[10].

- Processing is necessary for compliance with a legal obligation (Article 6(1)(c)), for example, for accounting and regulatory requirements associated with purchases.

In principle, there is no hierarchy in establishing which legal basis to rely on for any given processing activity. It is the data controller's responsibility to justify the appropriate legal basis for each processing activity.

A fundamental early task is to distinguish between features that require the processing of personal data, and which are strictly necessary to run the game, and those that are optional, supplementary, or monetisation driven. After all, the GDPR requires data controllers to base every processing activity on one of the six legal bases listed in Article 6 of the GDPR, and the criteria of necessity can influence the choice for one legal basis or the other. It also requires data controllers to identify the purpose of each processing activity before it begins. Once the legal basis and the purpose of any given processing activity are established, the personal data collected during said activity cannot, in principle, be further used in a way that is incompatible with the original purpose. For that, a separate legal basis would be necessary.

Many actors can face difficulties later in the lifecycle when they realise that personal data initially collected for "gameplay improvement" is being repurposed for targeted advertising or engagement-based monetisation. If such distinctions are not formally recognised during pre-production, function creep becomes almost inevitable, raising issues under the principle of purpose limitation. Properly documenting the purposes and the legal bases for each processing activity is therefore essential for compliance and should be implemented as early as possible at this lifecycle stage.

4.2.3 Supporting accountability, governance and proactive lifecycle management

The principle of accountability requires controllers to demonstrate not just compliance, but structured and documented compliance. A written data lifecycle map that shows how each data category enters the ecosystem, is processed, stored, transferred, retained, and deleted, serves as a central compliance artefact. Such documentation also supports better compliance with other requirements set out in the GDPR, such as:

- International transfer assessments under Chapter V[11].

- Internal governance under Article 24.

- Joint Controllership Agreements under Article 26.

- Data Processor Agreements and contracts under Articles 28–29.

- DPIAs under Article 35.

[10] EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en

A detailed lifecycle map helps development and live-ops teams maintain a shared mental model of the data they are responsible for creating, transforming, or safeguarding.

Concerning international transfers under Chapter V, it is essential that controllers identify server locations, adequacy decisions, Standard Contractual Clauses, and transfer risk assessments as early as possible in the game lifecycle to prevent non-compliant design and architectural choices that are difficult to correct later.

It is essential to acknowledge the "Russian dolls" effect in video games, the nested chain of SDKs where integrating one primary development technology automatically pulls in multiple sub-SDKs from third parties, creating opaque layers of data processors that controllers often cannot easily map or control. They need to mandate full sub-processor manifests from their processors and reject "black box" mediation. They should require prior controller notice/approval for sub-changes (Article 28(2)) and establish limits, for example, "no dolls beyond 2 levels". It is recommended to use SDK scanners and similar tools in CI/CD[12] to map nests in this lifecycle stage. And fallback to direct integrations or local-first (no-cloud ads, for example) for default configurations. Furthermore, development technology providers should design their services so that functionalities (audience analytics, advertising retargeting, etc.) are decorrelated, allowing clients to select only the software modules they need to minimise all these integrations.

Hardware suppliers should clearly mark in dev kits and documentation which telemetry flows are under their control, and which are provided as "pipes" for publishers. For joint dashboards, they should add a short "joint controller" section in partner contracts that covers the legal bases, transparency duties, data breach responsibilities, and handling of data subjects' rights. In addition, they should classify each behavioural inference (e.g., churn prediction) by potential impact. For example, UX optimisation, monetisation targeting, or safety, building specific DPIA sections as soon as high-risk scenarios are identified. The flag "children involved" is crucial at this stage too (see section 4.4.1 later).

If you are a creator, designer or developer, for each account store (QA tools, bug trackers, alpha/beta portals), you should record the purpose, who decides content and retention, and whether you reuse it. Where you are the processor, refuse "verbal only" instructions, require written instructions, including retention and deletion on project end. In each analytics plan, tag each event with: "publisher only" vs "studio reuse". The latter requires your own legal basis and records of processing. For external playtests, prepare a "telemetry notice" template that explains what is recorded during tests, who sees it, and how long it is retained. This information must be aligned with publisher's notices. Finally, when scoping AI/personalisation features in preproduction, add a short "Profiling role sheet" per model: who owns it, who can reuse it, and whether you are the controller or the processor. For high impact mechanics later in the game lifecycle (e.g., dynamic pricing, engagement maximisation for minors), suggest the publisher to conduct a joint DPIA.

Development technology providers should separate "tool user" accounts (for dev teams) from "player" accounts created via their service. They should provide template wording so game studios

[11] EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf

[12] CI/CD (Continuous Integration and Continuous Deployment/Delivery) is a DevOps methodology that automates software building, testing, and releasing.

can clearly explain whether they co-control authentication (e.g., "X authenticates your account on our behalf"). These providers should provide a dataflow diagram per product that explicitly lists data fields, recipients, controllership, and configuration options. Additionally, they should offer standard contract clauses: "You (studio) are controller for X; we (provider) are controller for Y telemetry; for Z, we are your processor under these instructions". It is strongly recommended for them to publish a detailed "profiling data sheet" for each behavioural module, including inputs, outputs, purposes, the controller, and how data subjects can exercise their rights.

During preproduction, publishers should decide whether the game will use platform-only accounts, publisher accounts, or a hybrid, and run a quick role checklist for each. For alpha/beta signups, they should keep a separate registry entry recording what data they collect (emails, age, platform IDs) and whether they will later use it for marketing or future titles (in this case, they will be the controller for this processing). In alpha/beta agreements with testers, publishers must specify whether telemetry is anonymised/aggregated and whether it will feed future titles or profiling, adjusting transparency and choice mechanisms accordingly.

For storefronts, when setting up alpha/beta programmes through the store, they need to clarify in contracts which consents/notices the store shows, what data the publisher receives, and under which role (independent controller vs processor). They should provide a "role one pager" for each programme to publishers, so both sides can align privacy notices or DPIAs. They should provide publishers with a clear "telemetry role guide" distinguishing store analytics (their controllership) from per game analytics (under the publisher/studio controllership). Finally, for each recommendation/targeting model, they need to document which data sources are used (for example, store behaviour only vs in-game telemetry).

4.3 Conceptualising and designing game mechanics

4.3.1 Embedding data protection by design and by default

Article 25 GDPR requires controllers to integrate data protection safeguards "both at the time of the determination of the means for processing and at the time of the processing itself"[13]. In the gaming context, this obligation is profoundly relevant to the conceptualisation of how a video game is designed. By the time games are beginning to be refined, many choices regarding data flows, player profiling, and backend architecture have already been made. The data protection by design must, therefore, be in the minds of those who handle the game's operational as well as creative design. For creators, designers and developers, this principle is therefore a creative constraint that defines which mechanics are permissible without disproportionate processing of players' personal data. A game designer deciding whether progression must be tied to persistent identifiers, for example, is making a privacy decision just as much as a narrative or systems decision. If achievement validation or skill assessment can be performed locally (e.g. via device-stored data) rather than through continuous telemetry uploads, the design must favour the less intrusive option.

In practice, treating privacy as a core design parameter often leads to the adoption of alternative, privacy-friendly approaches, such as aggregated or session-based matchmaking tiers instead of detailed behavioural profiles or technical separation of the logs needed for security/antifraud (strict necessity) from other logs used for UX or marketing, for example.

[13] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

Local processing in video games perfectly embodies GDPR Article 25's data protection by design and by default by minimizing data transmission to servers, reducing exposure to breaches, and limiting centralised profiling across the ecosystem. Good examples are local progression systems for offline or single-player genres, reducing reliance on persistent uploads to an online server via accounts and on-device computation for VR or motion-tracking features, minimising the transmission of potentially sensitive behavioural signatures.

This approach embeds protection from the outset, with no server transmission: personal data such as telemetry or even basic behavioural inferences stays device-bound, eliminating significant risks during collection and initial use. Only aggregated or strictly necessary results reach servers, avoiding bulk uploads of raw personal data. Processing occurs under user-owned and controlled hardware, giving players inherent oversight. This should be the default for sensitive features, new updates or games should ship with local-first logic, making "local" the baseline unless the player opts into cloud syncing.

By default, optional account fields, social-graph features, and third-party data sharing must be set to "off", requiring explicit action for activation. In practice, this means that optional analytics should not be silently enabled after account creation, multiplayer discovery settings should default to private or friends-only where feasible, and features including behavioural personalisation should have to be activated by an explicit opt-in, for example. In addition, a good practice is to default lapsed players re-engagement to maximum privacy settings (no cross-title profiling, no shared friends): a player returns to a platform after a year; instead of being instantly shown to all friends, auto-added to cross-game "recently back" lists, and profiled across every title they own, they re-enter in a "quiet" mode by default where their presence is mostly private unless and until they explicitly switch on more social and personalised features. Development technology providers should ensure that their SDK dashboards display only aggregated metrics. Accessing raw, player-level telemetry must require a time-bound, logged privilege escalation process not accessible for everyone. During instrumentation, publishers should mark individual telemetry events as "essential" versus "non-essential" to ensure that privacy controls can disable the latter for players. Hardware suppliers and development technology providers should offer configuration flags allowing clients to disable profiling features entirely, for example, in specific geographic regions. Profiling tools should be modularised, ensuring that profiling data collected for the purpose of safety or skill-based matchmaking is strictly separated from profiling data collected for monetisation purposes to prevent the exploitation of player vulnerabilities. In general, development technology providers should offer configuration flags that allow studios to disable high-risk uses (e.g., for children) and document these as part of "data protection by default" measures. Furthermore, storefronts should architect their systems so that sharing identifiers with publishers uses narrowly scoped tokens rather than full account records.

4.3.2 Integrating privacy into narrative and social design

Creators, designers, and developers increasingly integrate AI-driven NPCs to enhance immersion, dynamic storytelling, and personalisation. These NPCs often process player data, such as chat messages, voice commands, gameplay choices, and behavioural patterns, to generate responses, adapt narratives, or enforce moderation.

Every NPC feature that collects or infers player data must rest on a valid legal basis. Fairness demands avoiding discriminatory outcomes from AI models, so regular audits for bias in NPC decision-making, such as dialogue tailoring or reward allocation, help ensure equitable treatment across player demographics. Controllers need to disclose NPC data practices through contextual notices (for example,

tooltips explaining, “This AI remembers your choices to personalise quests”) and comprehensive privacy policies that detail flows, retention, and AI involvement.

NPC data processing should be strictly confined to predefined gameplay purposes, for example, real-time adaptation or anti-cheat detection, with code-level safeguards preventing drift into marketing or external analytics without an adequate legal basis. Controllers must complement this approach with data minimisation by capturing only essential elements. For example, summarising chat intents rather than storing full transcripts, and enforcing automatic purging of raw inputs post-processing.

AI-driven NPCs must prioritise accuracy by validating inferred player profiles against user feedback loops, allowing corrections via simple in-game interfaces to rectify errors in remembered preferences or behaviours. Controllers should pair this with storage limitation through tiered retention policies: ephemeral for session-bound data, short-term for cross-session continuity, and indefinite only for anonymised aggregates. To empower data subjects, NPC interactions and player menus should integrate seamless rights tools such as one-click memory resets, data exports, or objection forms. Finally, training AI-driven NPCs in games involves feeding models with player interaction data (chat logs, choices, voice patterns, etc.) to enable adaptive behaviours. In this case, recommendations for training other AI models would apply. An essential one is to rely on synthetic data when possible and to minimise the training dataset in the rest of the cases, by aggregating or pseudonymising inputs, replacing identifiers with tokens, and stripping unnecessary details such as timestamps or locations before feeding into models, ensuring only indispensable patterns (for example, dialogue styles) are retained. Pre-training audits are strongly recommended to verify that no direct or indirect identifiers persist.

Modern games increasingly incorporate persistent social spaces such as matchmaking lounges, guild halls, public lobbies, voice or text chat channels and rooms, trading environments, and user-generated content hubs. These systems enable player creativity and community building but also introduce substantial privacy risks. The inclusion of social features must therefore be approached with a clear understanding of the implications for purpose limitation, profiling, and fairness, particularly when minors are present.

The different actors should consider questions such as:

- Are social features truly optional, or will players be prevented from accessing core content if they do not engage with them?
- Will communications be moderated by automated means, stored persistently, or analysed for behavioural profiling?
- Do reputation or trust systems rely on extensive behavioural data that could unduly influence players’ experience or autonomy?
- Could unsolicited invitations, friend requests, or public interactions expose children to inappropriate content or manipulative behaviour? Are there parental dashboards or equivalent tools that allow guardians to disable voice chat, restrict friend invitations, or review communication settings?

Addressing issues such as these early in the game’s design prevents the creation of systems that would be technically or economically infeasible to modify later. It also ensures that safety considerations are not retrofitted but naturally integrated into the game’s world.

4.3.3 Avoiding deceptive and addictive design

Each actor that engages in telemetry or behavioural inference must ensure that their own interfaces and contractual arrangements do not enable or conceal deceptive or addictive design patterns, and that GDPR compliant choices propagate through the entire gaming stack.

Deceptive and addictive patterns such as manipulative consent flows, loot boxes timed to frustration, or nudges exploiting spending vulnerabilities often rely on telemetry data (play patterns, inputs, session lengths) and behavioural inference (churn risk, whale propensity). This infringes different GDPR principles and requirements, including Articles 5, 9 and 25[14],[15]. Controllers need to design privacy interfaces with equal friction for accept/refuse, avoiding pre-ticked boxes, confirmshaming ("Decline and lose rewards?"), or disguised opt-outs. They must clearly separate, for example, consents for core gameplay telemetry from monetisation profiling and avoid using inferences to personalise pressure (e.g., offers during losing streaks), as this undermines fairness and risks invalidating consent across the chain.

In addition, controllers must collect only telemetry essential for the stated purposes, separating "safety/analytics" data from monetisation models. They need to constrain profile windows (e.g., the last 3 sessions) to prevent lifetime dossiers and explicitly prohibit deriving/storing weakness or vulnerability inferences (e.g., addiction signals, financial stress) for engagement tuning, as these approximate special category data under Article 9. Publishers and storefronts are in a privileged position to prevent harmful design; they may, for example, incentivise creators, designers, and developers not to use addictive design patterns that make players want to keep returning, often by combining fast rewards, progression, social pressure, scarcity, and personalised goals.

Loot boxes are another major concern. A loot box is an in game "mystery package", a consumable virtual item that hides its contents until opened; the player knows only the possible types or rarities of items (common, rare, epic, etc.), not the exact outcome (cosmetics, weapons, card pack style rewards, etc.). They can be earned in gameplay or bought directly, and many systems use visual cues (lighting, colour-coded rarity) and "pity timer" mechanics to encourage players to keep opening more loot boxes. Loot boxes rely on variable rate reinforcement, the same principle that underlies slot machines: rewards are unpredictable, which strongly activates the brain's reward system and makes players keep trying "one more time". This can interact with traits such as impulsivity, need for novelty, or gambling tendencies. If they are not fully regarded and regulated as gambling activities, controllers must ban these boxes for minors and make them optional for the rest of the players (for example, with "buy direct" options next to the random boxes). When players do engage with loot boxes, full transparency and disclosure of information such as drop rates and spending statistics is required.

Additionally, cosmetic systems such as skins, clothes, and avatar customisation are especially concerning because they can contribute to that pull by strengthening identification with the character and making self-expression feel meaningful. In simple terms, when a player feels connected to their in-game character on a sentimental level, i.e. "this character is a virtual extension of me", changing its appearance can become an emotionally rewarding experience rather than a purely aesthetic one.

[14] EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[15] AEPD Report on addictive patterns in the processing of personal data: Implications for data protection, https://www.aepd.es/guides/addictive-patterns-in-processing-of-personal-data.pdf

Cosmetics can become especially engaging when they are tied to progression, limited-time events, rarity, social visibility, or status signalling. That means a skin is not just a visual choice; it can also signal prestige, belonging, taste, or achievement, which can make players repeatedly chase new looks.

Understanding players' motivations is also important. Different players can be drawn in for different reasons. Some enjoy self-expression and experimentation, some want to match a preferred identity, some want recognition from other players, and some are motivated by completionism or fear of missing out when cosmetics are offered only for a limited time. Common patterns that amplify engagement include rotating shops or seasonal items that create urgency, rare or exclusive skins that create status pressure, progression tracks that reward repeated play with cosmetic unlocks, social display systems, such as emotes, lobbies, profiles, ranked badges or bundles and microtransactions that nudge repeated spending or collection behaviour. The concern is not that cosmetics or similar design features are inherently harmful. The concern is that when combined with strong reinforcement loops, monetisation pressure, and scarcity tactics, these practices may exploit vulnerable players, especially those who are younger, highly status-sensitive, or prone to compulsive spending or repeated play. This is the reason why UX testing for deceptive and addictive patterns is strongly recommended via independent audits before release.

4.4 Anticipating risks, with a special emphasis on children

4.4.1 Conducting a DPIA for high-risk personal data processing

A DPIA is a process designed to describe a personal data processing activity (or multiple processing activities that are similar), assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from this processing by assessing them and determining the measures to address them[16]. DPIAs are important tools for accountability, as they involve a process for building and demonstrating compliance.

In line with the risk-based approach of the GDPR, conducting a DPIA is not mandatory for every processing operation. A DPIA is required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons". Some examples are the evaluation or scoring (including profiling and predicting), especially from aspects concerning.

the data subject's performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements; automated-decision making with legal or similar significant effect; systematic monitoring; sensitive data or data of a highly personal nature (this includes special categories of personal data as defined in Article 9 GDPR); data processed on a large scale; matching or combining datasets; data concerning vulnerable data subjects; innovative use or applying new technological or organisational solutions and when the processing in itself prevents data subjects from exercising a right or using a service or a contract. The previous sections have already shown that several game features may involve high-risk processing activities under the GPDR following these criteria, thus requiring a DPIA before launch. Processing activities that may require a DPIA include extensive behavioural profiling, automated content moderation, anti-cheat decision-making, processing of children's data, processing of sensitive data gathered through sensors and BCIs, including biometric data, and location-based features.

[16] WP Article 29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whetherprocessing is "likely to result in a high risk" for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

The GDPR specifies the scope of a DPIA and the content it must include (Article 35 GDPR). When carrying out a DPIA, the controller must make sure that it includes a systematic description of the processing operations in question and their purposes. The controller must also assess the necessity and proportionality of the processing activity in relation to the abovementioned purposes, as well as the risks the processing activity may have on the rights and freedoms of data subjects involved. Finally, the DPIA must include an overview of envisaged measures to address the identified risks. If, after the assessment, the controller concludes that the residual risk remains high, Article 36 requires prior consultation with the supervisory authority.

DPIAs should not be seen merely as legal paperwork but as creative and technical tools useful for compliant and responsible game design. They often reveal that gameplay objectives can be achieved with less intrusive data processing. For example, by shifting sensitive computation to the device, reducing data retention periods, or introducing human oversight into automated moderation pipelines.

Even if the obligation to carry out a DPIA is not triggered, controllers must still implement measures to manage risks to data subjects' rights and freedoms. Furthermore, controllers must continuously assess the risks arising from their processing activities to identify when processing is likely to result in a high risk to individuals' rights and freedoms.

4.4.2 Recognising children's unique vulnerabilities in the context of data protection

Children are among the most active participants in gaming environments, and their presence fundamentally alters the controller's responsibilities. Under Article 5(1)(a), processing must be fair, and fairness for children requires heightened protective standards. Children may not fully grasp the scope and the risks of certain data processing practices, may be more susceptible to deceptive or addictive design, and may face increased exposure to harmful interactions in social or multiplayer environments.

Unless a game is clearly and demonstrably exclusively targeting adults, all industry actors must assume that children will be present and make their decisions accordingly. The gateway to any game must be designed with age-appropriate considerations. During the conceptualisation of account systems, the different actors must design flows that support verifiable parental consent, and/or age assurance[17] when necessary. It is good practice to test these with mock UX flows during pre-production to ensure they are effective before implementation.

Furthermore, creators, designers, and developers who recruit minors for early playtests must specify an age threshold and create separate parental consent forms with verifiable logging, ensuring these records are stored alongside the tester's account ID for accountability.

Article 8 GDPR introduces a further requirement: when consent is relied upon for children below the age at which they can give valid consent, parental authorisation must be verifiable. A well-designed parental consent mechanism balances two competing demands: it must be sufficiently reliable to enable parental consent to be verified with a proper level of certainty, but it must also be proportionate, so it does not require intrusive identification. Common approaches include sending a one-time verification code to a guardian's email address, using a tokenised payment card check without storing card information, or using a parental dashboard that requires a guardian to explicitly approve the child's participation.

4.4.3 Crafting age-appropriate interfaces

Articles 12, 13, and 14 of the GDPR require that privacy information be provided in a manner "easily accessible and easy to understand", with special adaptations for children. In practice, this involves designing transparency interfaces that reflect players' cognitive abilities. Simplified explanations, visual illustrations, concrete examples ("We save your progress, so you don't lose it"), and consistent terminology across menus all contribute to meaningful comprehension. When separated by age, the version for the children's experience should, by default, conform to the applicable recommendations in age-appropriate design codes. In the case of default protection, all users are treated the same way because their age is unknown, nor is it known whether they are over a certain age. The code's standards should be applied to all users, ensuring that minors are consistently exposed to a design suitable for them.

This ensures that their needs are respected, and their best interests are protected. Adults who assure their age can modify this interface or default settings. This approach can benefit users with less digital competence, specific disabilities or older people, to mention just a few examples. All users (not just children) should have the option to voluntarily access different design versions of the interfaces and transparency notices according to their needs and preferences. This adaptive design does not necessarily have to be based on age verification processes, but rather on giving users options to freely choose the ones they believe are most suitable, useful, or beneficial. The goal is not merely stylistic clarity; it is to ensure, for example, that consent is valid if relied upon.

4.4.4 Identifying high-risk features for children and architecting for child safety

Certain game features carry heightened inherent risks when used by children, including public communication channels, friend recommendation algorithms, location-based interactions, camera-based AR mechanics, identifiable avatars, and (untransparent) microtransactions such as loot boxes. Creators, designers and developers must assess whether these features are compatible with a child's best interest and what additional safeguards may be needed. Child safety must be embedded into the game's design and architecture. Creators, designers and developers may implement restricted communication modes, automated filtering, guardian dashboards, spending limits, time-of-day restrictions, or accessible reporting tools. These design decisions reinforce safety, privacy, and GDPR compliance simultaneously. At the system level, storefronts and launchers should plan to restrict generic accounts to default features and disable social functions by default, linking these restrictions directly to age gates in the data model. Only adults should be able to change this kind of safe configuration.

One of the most significant magnifications of risk for children occurs in behavioural profiling (and advertising). In this sense, all industry actors should adopt a "safe-by-default" approach unless the game is only available for adults. Hardware suppliers should explicitly disable monetisation-focused profiling for generic users who do not demonstrate they are above a required age threshold. Development technology providers should design their service to accept and process an age signal so that features can be restricted/enabled automatically depending on the assured age and support this good practice. Creators, designers and developers including minors in playtests, must avoid profiles that measure or exploit spending or compulsion, limiting their analysis to usability and frustration patterns that drive design improvements.

[17] EDPB Statement 1/2025 on Age Assurance, https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf

Publishers must ensure that only accounts marked as “adult” can enable monetisation-oriented profiling. Finally, storefronts should set “no personalised marketing” as the default for generic accounts and ensure that recommendations for these users are limited to non-profiling suggestions such as editor’s picks. In general, for games accessible to young audiences and popular with them, all actors should actively flag and review any profiling models aimed at maximising monetisation or engagement considering alternative goals (satisfaction, well-being). Development technology providers should include contractual clauses that forbid clients from passing “known minors” labels into profiling APIs without additional agreed-upon safeguards.

5. Recommendations and good practices during Release

This stage marks the point at which a game’s design philosophy becomes operational reality. GDPR concepts such as lawful basis allocation, fairness, transparency, data protection by default, or child protection, which may have remained theoretical during pre-production, must now materialise in practice in the interfaces, settings, user journeys, monetisation flows, and backend systems that potentially millions of players will encounter. Where pre-production requires imagination and structural foresight, the release phase requires discipline: the discipline to ensure that every feature, every onboarding choice, every data-collection practice, and every interaction align with the legal and ethical commitments the data controllers and processors have made.

Live operations add a further layer of complexity. Once players begin interacting with the game at scale, studios face continuous real-time pressures: feature rollouts, content patches, balancing cycles, emerging community norms, adversarial behaviour, automation needs, cyberattacks and monetisation strategy adjustments. GDPR compliance must not merely survive in this environment; it must remain stable and reliable, even under commercial pressures or rapid development cycles.

5.1 Identifying GDPR roles and responsibilities

Identifying these roles should have been done in the first stage of the game’s lifecycle, as it is a task that must be carried out during the preproduction and production stage, when all personal data processing activities are planned. However, all the guiding questions regarding the processing carried out once the video game is on the market are included here for clarity. Maybe some guidance questions in section 4.1 could be helpful too when determining GDPR roles under this section.

5.1.1 Hardware suppliers

Guidance questions:

- Are platform accounts mandatory to play the game or access online features, and do you set required fields, security checks, and cross-device linking rules? If yes, you are the controller for those accounts.

- Do you and a developer or publisher co-decide cross-account features (cross-progression, unified friends list, cross-title bans)? If yes, assess joint controllership.

- Do you expose a login solution that publishers can brand and configure, while you also reuse account data for your own analytics or marketing? If yes, you are independent controller for your reuse; the publisher is controller for their use, even if the same account is used.

- Are you collecting platform telemetry from all games (session time, performance, error reports, usage patterns) to optimise the platform, enforce policies, and recommend games? If yes, you are the controller.

- Do you share platform telemetry with publishers through dashboards you co-design (shared KPIs affecting both parties' decisions)? If yes, examine joint controllership for that shared analytics service.

- Do you build cross-game profiles of players' habits or skills across the hardware platform to recommend titles or adjust moderation/anti-cheat thresholds? If yes, controller for those inferences.

- Are you sharing segments ("high spender," "competitive player") with publishers for their own campaigns? If yes, distinct controller roles: assess whether you are joint controllers for shared campaigns or separate controllers exchanging data.

In summary, per data processing activity type:

- Account creation and management (hardware platform account): likely controller, sometimes joint controller or processor.

- Gameplay monitoring (platform telemetry): controller, joint controller when telemetry is co-used with publishers.

- Behavioural inference (platform-level inferences): likely controller.

5.1.2 Creators, designers and developers

Guidance questions:

- Does the game expose a sign-up or in-game account interface under your studio brand, with your own privacy notice? If yes, you are controller for that account.

- Are you running accounts solely on behalf of a publisher (publisher brand, publisher privacy notice, publisher decides fields and reuse? If yes, you are the processor for that account processing.

- Do you retain test (early access player) accounts into Release and reuse them for community or analytics? If yes, you are the controller.

- Who decides which telemetry events are instrumented (e.g., level completion, button presses, chat events) and why? If you decide or co-decide beyond technical necessity, you may be controller or joint controller.

- Will you store telemetry in your own environment and reuse it across titles to improve design, balancing or AI models? If yes, separate controller.

- Are you contractually obliged to collect and forward raw telemetry exactly as specified by publisher, with no independent reuse? If yes, processor.
- Are you designing or tuning live models for matchmaking, dynamic difficulty, or personalised content directly in your live-ops loop, for your own titles? If yes, controller.
- Are you implementing profiling logic entirely as specified by the publisher, on their systems, with no reuse across games or clients? If yes, likely processor.

In summary, per data protection activity type:

- Account creation and management (game accounts): controller for own test accounts; processor if accounts are managed for a publisher.
- Gameplay monitoring (game telemetry): processor when collecting telemetry solely for the publisher, controller when using data for own R&D across projects.
- Behavioural inference (game-level inferences): controller when building models for own purposes, processor when building models solely for publisher under instructions.

5.1.3 Development technology providers

Guidance questions:

- When players log in with your identity management service (e.g., engine-linked account), do you set terms of use and reuse data across games? If yes, controller for that account.
- If a publisher mandates your identity management service but restricts you from reusing data and you work strictly under their documented instructions, are you limited to technical authentication? If yes, you may act as processor for that specific flow.
- Does your service automatically send telemetry to your servers from every live game (e.g., performance, device info, crash details) for your product improvement and research? If yes, controller for that processing.
- Can studios configure telemetry to stay fully local or to go only to their endpoint? If they choose your endpoint, but you reuse high-level aggregates across customers, you still act as controller for that reuse.
- Are you providing a hosted analytics stack where the publisher defines events, metrics, retention, and you are contractually bound not to reuse data? If yes, you may be processor for that stack.
- Are you offering generic churn, engagement, or monetisation prediction services across many games, trained on cross-client data? If yes, controller for that profiling, even if studios are also controllers when they apply the obtained predictions.
- Are you and specific clients co-defining segmentation criteria and campaign rules using your engine? If yes, assess joint controllership.

- Are you merely providing a hosted environment where the client uploads data, defines models, and you neither see nor reuse the data? Then for that activity you may be closer to processor or even outside controller/processor scope regarding end-user data.

In summary, per data processing activity type:

- Account creation and management (own service accounts): controller, processor if purely authenticating for a client.
- Gameplay monitoring (service telemetry): often controller, sometimes joint controller; may be processor if truly instruction-bound.
- Behavioural inference (service-level inferences): controller for generic behavioural models (possible joint controller), sometimes processor.

5.1.4 Publishers

Guidance questions:

- Are you running publisher-wide accounts that connect multiple games, platforms and devices, and define all purposes (cross-title analytics, offers, bans)? If yes, controller.
- Are loyalty programmes, cross-game progression or combined ban lists co-designed with platforms or storefronts? If yes, determine if this a joint controllership or separate controllers exchanging data (it depends on architecture and data flows).
- Are you defining live KPIs (churn, difficulty, monetisation, toxicity) and deciding what telemetry events each build sends to live servers? If yes, controller.
- Are you combining platform telemetry, store telemetry, and in-game telemetry into unified player views? If yes, you are clearly controller.
- Are you relying on vendor dashboards where both you and the vendor decide what segments or triggers to use (e.g. promotions based on real-time behaviour)? If yes, consider whether this is joint controllership.
- Are you building or commissioning models to segment players for offers, events, difficulty, or retention strategies across your portfolio? If yes, controller.
- Are these models co-designed with platforms or stores (e.g., joint retargeting across several surfaces)? If yes, examine joint controllership for that specific programme.

In summary, per data processing activity type:

- Account creation and management (publisher accounts): controller, sometimes joint controller with creators, designer and developers.
- Gameplay monitoring (publisher telemetry): controller for telemetry, joint controller with other actors where they co-decide.

- Behavioural inferences (publisher-level inferences): controller for gameplay-based profiling, sometimes joint controller with hardware suppliers/development technology providers/ storefronts.

5.1.5 Storefronts

Guidance questions:

- Are store/launcher accounts mandatory for using social features, purchases, and cloud saves, and do you reuse them across many games? If yes, controller.
- Are there co-branded "publisher hubs" where you and a publisher co-decide membership criteria and benefits (e.g., VIP tiers across several games)? If yes, assess joint controllership for that club.
- Are you tracking installed games, play frequency, session length, navigation in the launcher, and purchases to improve the store and personalise recommendations? If yes, controller.
- Do you give publishers access to store-side telemetry (impressions, clicks, conversion) that you both use to optimise promotions? This can still be separate controllership, but co-designed targeting may indicate joint control for that promotion.
- Are you profiling players based on purchases, wish-lists, playtime, and browsing to recommend games and surface offers? If yes, controller.
- Do you run joint campaigns where you and a publisher co decide targeting rule (e.g., "show this bundle to segment X at time Y") using shared data? If yes, likely joint controllership for that campaign.

In summary, per data processing activity type:

- Account creation and management (storefront account): controller, potentially joint controller with publishers for co-branded programs.
- Gameplay monitoring (storefront telemetry): controller for telemetry used to run and optimise the store/launcher, joint controller if co-deciding on telemetry with publishers.
- Behavioural inference (storefront-level inferences): controller for own recommendation and ad-targeting systems, sometimes joint controller with publishers for joint campaigns.

5.2 Protecting personal data while playing

5.2.1 Embedding transparency in the player experience

When players first boot up a game, they must be able to understand, in clear and contextualised terms, how their personal data will be processed. Articles 12,13 and 14 GDPR require that information be concise, intelligible, and easily accessible, but they do not dictate a specific format or form in which the information must be provided. Games, therefore, have enormous creative scope to embed

transparency into the player's experience, rather than relegating it to static legal text hidden in different privacy notices and locations.

A well-designed onboarding flow introduces privacy concepts gradually. This often begins with a short, human-readable explanation of the essential facts: that certain personal data will be processed to create an account or enable progression, that optional features may require additional permissions, and that players can revisit and change their settings at any later point in time. By integrating transparency within the natural rhythm of onboarding processes rather than disrupting them, the different ecosystem actors avoid overwhelming players while still respecting their rights.

Consider creating "privacy labels" playing for data practices the same role PEGI[18] plays for game content: a standardised, glanceable signal that helps people make faster, better-informed decisions at the exact point of choice (storefront pages, install screens, update prompts, etc.). PEGI already shows that the videogame ecosystem can successfully use a compact, color-coded, widely recognised format to simplify complex risk information for players and parents. In general, simplified and visual presentation methodologies are recommended. In particular, controllers should consider the specificities of the devices used to play and of interfaces, for example regarding limitations in terms of available space. Privacy labels would not replace fuller notices, just as PEGI does not describe every aspect of a game. Rather, the label would function as a front-end layer of clarity, while the underlying detailed disclosure remains available for players who want it.

In this sense, the most effective transparency mechanisms anticipate context. For example, if a player tries to enable voice chat for the first time, the relevant transparency information should appear immediately, rather than being buried in a menu. Similarly, if the game offers personalised recommendations or location-based events, the interface should explain what data is required and why at the point where the feature becomes relevant. Transparency thus becomes an ongoing dialogue rather than a one-time notification that is often ignored and then forgotten about.

Additionally, it is good to link each data item to its legal basis (contract for core ID, legitimate interests for fraud flags, consent for marketing flags, etc.) when deploying this kind of "live" privacy notice. Use clear language in messages, screens and interfaces (e.g. "We need your email for game saves – processing is necessary for the performance of a contract") and always provide links to layered privacy information.

Actors interacting more frequently and explicitly with players such as Publishers or Storefronts (also Hardware suppliers) should deploy dedicated Privacy Centres or Hubs to centralise all information, transparency mechanisms, and tools (see section 5.3 later). Collaboration among the different actors in the ecosystem is required to ensure that players have clear information on "who is who". Transparency mechanisms should explicitly cover technology, game, and platform integrations, identifying controllers in typical patterns (e.g., for account data: "When you use your X account to log into Y Game, X is the controller for your account and Y is the controller for your game data"). Avoid vague "trusted partners" wordings; provide players with clear information in a way they understand which data will be shared, for what purpose and with what legal basis, etc. Create and publish Telemetry catalogues, including information on events, fields, recipients, and uses.

[18] PEGI (Pan European Game Information) is the harmonised, centralised labelling European age-rating scheme for video games. It uses age categories and content descriptors to help players and parents quickly understand whether a game is suitable and what kinds of content it contains, https://pegi.info/

Loot boxes and other chance-based mechanics have become a regulatory focus across Europe. Where these mechanics involve personal-data processing, transparency obligations require that players be informed, for example, of the probability of receiving different rewards, and this information must be presented before a purchase, not concealed in a remote or otherwise difficult to find or access policy. If probabilities change dynamically, for example, increasing the chance of rare rewards after repeated purchases, the player must be informed of this.

5.2.2 Obtaining valid consent

At release, controllers must implement robust, player-facing consent mechanisms that meet the requirements for valid consent under Articles 4(11) and 7 GDPR. Valid consent implies consent that is freely given, specific, informed and unambiguous. These consent mechanisms serve as the critical gateway for all personal data processing relying on this legal basis. This stage sets the tone for trust and compliance, requiring granular, unbundled banners presented before gameplay begins, with clear explanations of telemetry collection, profiling, and third-party sharing tied to specific purposes like analytics, social features, or monetisation. Again, messages, menus and interfaces need to be adapted to make windows legible in different devices and environments, paying particular attention to accessibility issues.

Controllers should use onboarding clickwraps to block progression until consents are captured, relying on layered notices. For example, “High telemetry: sessions + inputs shared with 3 ad partners”, followed by expandable details on data flows and withdrawal rights. Choices need to be presented in a granular and balanced way, with separate toggles for categories. For example, “Analytics (essential)”, “Personalised ads (optional)”, “Cross-title profiling (opt-in)”. Ensure that “Reject All” is as prominent and frictionless as “Accept”, without denying core gameplay features. Provide context and let players preview consequences, avoiding jargon and testing for comprehension via usability studies. For example, “This enables loot recommendations based on your playstyle—your personal data stays local unless you consent to sharing”.

Controllers can rely on different mechanisms to keep the player informed proactively. For example, in-game notifications can be used to trigger pop-ups or banners for setting changes (e.g., toggling from private-by-default sharing to public), new features collecting telemetry (e.g., “This update adds behavioural tracking for personalised ads—review/opt-out?”), or inference-based monetisation (e.g., loot box nudges). Push alerts may also be useful to send device notifications for high-risk events, like account data shared with third-party ad-tech or post-update privacy impacts, with one-tap undo options. Inline warnings allow different actors to embed real-time flags during gameplay or menus, e.g., “Enabling voice chat shares mic data—confirm?” or “DLC install modifies analytics retention—details”.

Finally, controllers can offer user-accessible, live-view logs of personal data processing modifications (e.g., “Setting changed 10:56 AM CET: telemetry enabled”), exportable for portability. Furthermore, controllers need to log all interactions (timestamp, device ID, choices) in tamper-proof records for audit purposes, keeping in mind the principle of accountability (Article 5(2) GDPR). Additionally, they need to activate parental consent logging for child testers, early access players and the rest of players under the age threshold.

5.2.3 Ensuring purpose limitation and data minimisation during gameplay

All actors participating in the ecosystem should create a live account schema or dictionary and run verification scripts to guarantee that it is updated properly. Social fields should be opt-in only during players' onboarding, and free text profile fields should be replaced with controlled vocabularies (dropdowns, checkboxes). Controllers should configure automatic purging of inactive accounts after a fixed period (triggered by last login timestamp), always with prior notification to the player (for example through an email to the address linked to the account). They should also deploy automated and granular retention procedures, for example, core account data 5 years post last login, marketing data 12 months unless renewed consent. In general, it is recommended to periodically run verification scripts to guarantee that all planned data protection by design and by default measures are deployed properly after release.

During gameplay, personal data is generated continuously. Even in simple games, telemetry and inferences constitute rich sources of personal data. In complex multiplayer environments, the volume and granularity of data are even greater. Article 5(1)(b)'s principle of purpose limitation requires that this continuous flow of data be tied to the specific, explicit purposes identified in the pre-production stage. Controllers of these processing activities should lock a production telemetry and inference schema or whitelist, enforce this predefined schema and reject updates or hotfixes that add undocumented or arbitrary events or attributes. They should also explicitly limit profile windows (the temporal slice of that telemetry used to build or refresh the inferences) and deploy automated retention procedures, distinguishing between raw data, inferences or profiles, and aggregates. Finally, they should periodically try to prune data schemas, simplifying or trimming their personal datasets by removing unnecessary, redundant, or unused elements like fields, attributes, or inferences.

With regard to the principle of data minimisation, it is worthwhile to regularly review various aspects of any given processing activity, such as the volume, precision, and frequency of telemetry collection, against the actual needs of their declared purpose. Controllers should conduct a purpose–necessity check, documenting whether the collection of particular bits of personal data is necessary for the declared purpose.

The temptation to exploit gameplay data for new purposes grows rapidly once a game becomes commercially successful. Different actors may wish to reuse telemetry originally collected for debugging to build personalised functionality and offers; product teams may want to analyse behavioural patterns for retention forecasting. However, as discussed before, unless the original transparency notice anticipated such uses, or unless a compatibility assessment under Article 6(4) supports them, controllers must identify a new legal basis. Without this step, data reuse becomes unlawful.

5.2.4 Aligning monetisation mechanics with GDPR principles

Controllers need to clearly distinguish between data strictly necessary for game delivery and data used to optimise monetisation (personalised offers, "whales" targeting, lookalike audiences), which, in practice, often requires granular, opt-in consent. If the game generates targeted offers or dynamic pricing based on past behaviour, then the data supporting such decisions must be collected and processed lawfully. Furthermore, it is recommended to explicitly record every instance where users (or devices) are categorised into behavioural segments based on telemetry or inferences.

Monetisation models such as microtransactions, subscription layers, virtual economies, or cosmetic sales must be compatible with GDPR principles, particularly fairness and transparency under Article 5. Controllers must avoid mechanics that track frustration or cognitive bias or try to exploit specific weaknesses; this may be characterised as manipulative profiling (related to addictive design patterns) rather than fair data processing. Monetisation design must not rely on opaque psychological profiling that players cannot reasonably expect or understand, particularly when it impacts minors and vulnerable groups.

Controllers should go beyond generic "we improve our services" language and explain, in plain terms, what telemetry is collected (events, session data, device, social graph), which monetisation inferences are drawn (e.g. churn risk, high spender propensity, engagement vulnerability) and how they are used.

They must avoid purpose creep. For example, a studio might analyse a player's engagement with a particular game mode and then offer a unique cosmetic item related to that mode. If the personal data used to generate that offer was originally collected solely for gameplay balancing, repurposing it for monetisation may be unlawful without renewed valid consent.

Additionally, telemetry initially collected for security or quality must not be silently repurposed into cross title, cross device monetisation profiles, especially when shared across actors in the ecosystem. Contractual and technical separation should be implemented: HW/OS level telemetry, game level telemetry, and storefront analytics should be siloed, with explicit agreements and auditable interfaces when data is combined for monetisation.

Controllers must use the minimal telemetry necessary to achieve a given monetisation objective (e.g. recent spend history and coarse progression, rather than full clickstreams, detailed timings, or raw communications). Furthermore, they must constrain the temporal window of data used for monetisation inferences (e.g. last sessions rather than full lifetime), and aggregate where possible; this reduces identifiability and the depth of behavioural exploitation. They should avoid unnecessary sensitive inferences, not deriving or storing attributes such as addiction likelihood, mental health status, or financial stress solely to optimise revenue.

On the other hand, behavioural inferences in monetisation (e.g. churn risk, "high value" status) must not be treated as static truths. Controllers should implement mechanisms for regular model refresh and bias checks, for example.

Controllers also need to actively monitor and govern product placement (embedded branded items), dynamic ads (personalised banners, loot), and sponsorships (branded events, skins) to avoid unfair processing. It is also a good practice to support players well-being by building in checkpoints, autosaves, and natural breaks (session timers, "rest suggested" prompts) to curb over-engagement.

5.3 Facilitating the exercise of data subject rights through player-centric interfaces

5.3.1 Easy exercise of data subjects' rights

Actors participating in the ecosystem should maintain a role matrix per account type (dev account, tester account, player account, etc.) and data processing activity that specifies who is the controller/

joint controller and who answers data subject rights requests. However, the exercise of GDPR data subjects' rights can only be effective when it is accessible, intelligible, and integrated into the same environments where data subjects (players) make decisions about their personal data. In many non-gaming digital services, rights are exercised through web forms or email requests. In the context of a video game, however, such approaches can feel disjointed, slow, or inaccessible, particularly for players who primarily interact with the game through consoles or mobile devices rather than via a web interface.

For this reason, controllers should treat data subject rights as a core component of player experience design. A rights interface should be located in the account settings or in a clearly marked "privacy" or "personal data management" section within the main menu. It should not be buried behind multiple menu layers or require navigating away to external websites. Ideally, players should be able to access rights management across every platform where the game is available, including PC, console, and mobile. Embedding rights in familiar, game-native interfaces avoids unnecessary friction. It also strengthens the fairness and transparency principles in Articles 5(1)(a) and 12 GDPR by ensuring that players do not feel intimidated or excluded from exercising their rights simply because the mechanisms have been hidden away or are hard to find, access or use.

Development technology providers should support data subject's rights exercise exposing all the necessary APIs to access, rectify, etc. personal data in their different locations. Additionally, controllers should deploy customer support ticketing systems to support data subjects' rights exercise requests and perform end-to-end testing with dummy accounts before release.

5.3.2 The right of access (Article 15)

The right of access entitles players to obtain confirmation of whether their data is being processed and, if so, to receive a copy of that data, along with information about the purposes, categories, retention periods, and recipients[19]. While access requests may seem straightforward in theory, video games generate unusually rich and heterogeneous data for each player. Alongside the more straightforward kinds of personal data, such as names or email addresses, telemetry, communication logs, behavioural histories, matchmaking classifications, progression states, transaction records, and moderation outcomes will likely all fall within the scope of personal data.

For this reason, controllers must carefully design their access procedures. An access request should not produce an overwhelming or unintelligible dump of raw technical logs to be handed over to the player. Instead, the response should be structured and comprehensible, with explanatory context where needed. A well-implemented rights interface may allow players to download structured data files directly from within their account settings, accompanied by narrative descriptions explaining each dataset. Where files are too large or complex, the interface may provide summaries with the option to request full exports through a supervised process. The goal is not merely legal compliance but enabling players to meaningfully understand what is happening to their personal data and how that shapes their gaming experience. For example, publishers should also provide simple in-game controls to access profile categories, at least at a high level.

[19] EDPB Guidelines 01/2022 on data subject rights - Right of access, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en

5.3.3 The right to rectification (Article 16)

We have already referred to the issues and risks associated to the processing of incomplete or inaccurate personal data. The right to rectification allows players to have such inaccurate or incomplete personal data that is being processed by the data controller corrected. In a video-game context, this typically applies to account details, profile information, display names, demographic information (where collected), or inaccurate records of in-game actions. It may also apply where an algorithmic classification (such as a skill rating, behavioural score, or toxicity flag) contains demonstrable errors. Controllers must design systems that can respond to rectification requests without compromising gameplay integrity or opening avenues for abuse. For example, a competitive ranking system may rely on performance metrics that cannot simply be "corrected", yet if a player's progression data has become corrupted or misattributed, a rectification procedure must exist. Clear guidance should be provided to players on which data can and cannot be rectified, and why.

For children, rectification becomes especially important. A child may rely on inaccurate assumptions about the meaning of data entries or may unintentionally provide incorrect account information; mechanisms for rectification should therefore be accessible, uncomplicated, and accompanied by explanatory text.

5.3.4 The right to erasure (Article 17)

Data deletion is one of the more commonly exercised rights among players. Article 17 GDPR provides data subjects with the right to have their personal data deleted under certain circumstances. Read in conjunction with Article 12 GDPR, it requires that erasure be simple, accessible, and free of unnecessary friction. In games, erasure often intersects with complex data sets related to progression, social graphs, purchases, and inventories. Nevertheless, the legal obligation remains clear: if a player wants to delete their data and no legal basis requires continued retention, the data controller must comply. The right to erasure requires a controller who has shared data with other parties to inform other controllers processing that data to erase any links, copies, or replications. The controller must take reasonable steps to notify these controllers of the data subject's request. A respectful erasure process begins with clarity. Players should be informed, in plain language, about what will happen when their data is deleted: whether their progression will be lost permanently, whether their communications will be removed or anonymised, whether purchase histories must be retained temporarily for legal reasons, and whether any elements (e.g., irreversible in-game transactions) cannot be unwound. Players should, in any case, also be informed whether particular categories of personal data will be retained after fulfilling the erasure request.

Erasure should not require players to contact support, articulate their reasons, or undergo repeated confirmation steps. It should, in principle, be as frictionless as the creation of the account itself. For children and, where necessary, guardians, the ability to initiate erasure through a parental dashboard must be available, reflecting Article 8's requirement that consent, and consequently also the withdrawal of said consent, remain under their control.
Development technology providers have an essential role when exercising this specific right, since they need to expose one or more APIs for clients to submit player deletion requests that affect telemetry and behavioural inference datasets.

5.3.5 The right to restrict processing (Article 18)

Restriction is often misunderstood or overlooked, but it can play a crucial role in interactive systems such as video games. A player may request that a particular processing activity is restricted when they

contest the accuracy of their data, when the processing activity is unlawful, but they prefer restriction to deletion, or when controllers no longer require the data, but the player needs it retained for, for example, future legal claims.

In a video game setting, restriction can temporarily halt non-essential analytics, pause automated moderation assessments, or freeze certain behavioural profiling processes while a dispute is being resolved. Controllers must design internal mechanisms to flag and isolate restricted data to prevent inadvertent use in ongoing operations.

Restriction also plays an important role in safeguarding players who believe they have been misclassified by automated systems, such as anti-cheat or toxicity-detection models. Temporarily pausing automated outcomes while reviewing the underlying data aligns with both GDPR rights and fairness principle.

5.3.6 The right to data portability (Article 20)

Data portability allows players to obtain their personal data in a structured, commonly used, machine-readable format and to transmit it to another controller, at least where processing is based on consent or contract (e.g., account creation, in-game purchases). This right applies to player provided data such as usernames, email, friends lists, playlists/favourites, purchase history, gameplay settings, activity logs (e.g., achievements unlocked, playtime per level), raw telemetry and user-generated content like shared clips or profiles. It may not apply to inferences (e.g., behavioural profiles like "churn risk"), third-party data, or non-personal content like save files unless uniquely tied to identifiable activity.

While direct "migration" between game ecosystems is rare in practice, portability can still serve important functions. For example, players may want to export their progression logs, historical match data, cosmetic inventories, or social graphs for use in companion applications, community tools, or e-sports analysis platforms. Direct transfer is required only if technically feasible (e.g., API compatibility between platforms), controllers should provide, always within their means, well-structured export formats with descriptive metadata and documentation explaining how the files can be interpreted. It is recommended to provide an explicit overview of portable data, the implementation of "export my data" buttons with previews in common formats, the testing of direct transfers for major storefronts, the use of short retention for raw logs to simplify exports and the coordination via contracts (publishers ensure storefronts or developers to propagate requests across the stack, etc.).

Properly implemented portability fosters openness in the gaming ecosystem and respects the autonomy of players who invest years into their digital personas. It must be clarified that portability does not erase data or override intellectual property or licence terms.

5.3.7 The right to object (Article 21)

The right to object is particularly important in the gaming sector because it applies to processing that is based on legitimate interest as a legal basis, which often includes processing for purposes such as analytics, personalisation, and safety-related behavioural modelling. When a player objects, the controller must cease processing unless it can demonstrate compelling grounds that override the player's interests, rights, and freedoms, or unless processing is required for legal claims.

In practice, this right could play a vital role in optional systems such as personalised functionality and offers, targeted retention efforts, recommendation engines, and cross-game profiling. If a player feels uncomfortable with specific telemetry or behavioural inferences, the game should enable them to opt out through an intuitive interface, after which processing must cease unless justified by a clear exception. Publishers and storefronts may deploy a central opt-out registry blocking telemetry or behavioural inferences across all their titles, with opt-out options persisting across reinstalls. Objection by design needs to be embedded in the game mechanics. Specific game features must be conceptualised as modular components. For example, a "rule engine" for applying profiles to adapt difficulty should be built so that if a player objects to profiling, the mechanic can be disabled without breaking the core gameplay.

Controllers must not interpret objections as mere preferences. Under Article 21, they carry legal force. Interface designs must therefore avoid the temptation to steer players away from objecting, particularly through deceptive patterns.

5.3.8 Automated individual decision-making, including profiling, in live environments

Under Article 22 of the GDPR players have the right not to be subject to solely automated decisions that produce significant effects on them unless certain conditions are satisfied. It must be considered that many core features in modern games are essentially "automated decisions". For these automated decisions, such as fraud blocking, anti-cheat sanctions or other player violations of terms and conditions, or matchmaking tiers, actors must establish in their internal specs how threshold logic transparency will be maintained and how human review channels will be surfaced. This is vital for development technology providers who must offer API-level support for rights fulfilment and document model logic so publishers can provide meaningful explanations to players. For example, providers who create the "engine user accounts" or "profiling services" must document their logic sufficiently so that publishers can provide players at different lifecycle stages with explanations of why they were targeted with a specific mechanic or offer.

A GDPR compliant system balances automation with human oversight. For example, automated moderation might flag likely abusive content, but final sanctions could be confirmed by a human moderator or at least subject to easy human review upon appeal by the data subject. For automated account suspensions (fraud, Terms of Service violations), controllers could implement an "appeal ticket" button in the suspension notice with a guaranteed 24/48-hour human review SLA (Service Level Agreement). Matchmaking systems can use personal data to determine player skill levels, but if the outcome has significant consequences for progression or access to rewards, the algorithm's logic must be explained in meaningful terms upon request. In general, for any automated moderation or decision (e.g., chat bans, exploit detection), controllers should create a workflow with a template explaining the decision criteria (to be sent by email or displayed in the user interface), the appeal process, and human review commitment.

6. Recommendations and good practices during Post-production

Once a game has been launched and has entered its live-operations phase, the nature of GDPR compliance changes significantly. During pre-production and release, compliance is largely anticipatory or incipient: the task is to design and deploy lawful data processing activities that respect data subjects' rights and freedoms. Once the game is live, however, compliance becomes operational. Every update, event cycle, system refactor, monetisation experiment, or community management initiative carries data protection consequences. At this stage, the challenge is not to forecast or assess risk but to manage it continuously, ensuring that evolving technology, community behaviour, and business priorities do not undermine the commitments established during the first lifecycle stages.

Games are dynamic. They grow, contract, change shape, and change purpose over time. Some titles operate for more than a decade; others undergo intense evolution during the first eighteen months and then settle into slower rhythms. Whatever the trajectory, controllers remain responsible for personal data processing until the moment retention ends, and the game's infrastructure is fully decommissioned. That responsibility extends across three major operational periods: ongoing updates and feature evolution, continuous data governance and security, and the legal and ethical requirements that arise when a game approaches end-of-life.

6.1 Identifying GDPR roles and responsibilities

Identifying these roles should have been done in the first stage of the game's lifecycle, as it is a task that must be carried out during the design/development phase, when all personal data processing activities are planned. However, all the guiding questions regarding the processing carried out once the video game is actually on the market are included here for clarity. Maybe some guidance questions in sections 4.1 or 5.1 can be helpful too when determining GDPR roles.

6.1.1 Hardware suppliers

Guidance questions:

- Do you keep platform accounts active to re-engage lapsed players with events, sales and seasonal content across many games? If yes, controller for that long-term account use.
- Are you co-running long-term loyalty programmes with publishers (shared statuses, cross-game rewards)? If yes, assess joint controllership for that programme.
- Do you continue collecting and analysing platform telemetry (session length, game usage, error logs) for ongoing performance tuning, OS updates, and store optimisation? If yes, controller.
- Are long-term telemetry dashboards for publishers co-designed, influencing both your and their decisions (e.g., content positioning, feature support, updates)? If yes, examine joint controllership for that analytics service.
- Do you maintain long-term engagement profiles across many games to push events, subscriptions, and bundles? If yes, controller.

- Do you share segments ("sports fans", "heavy spenders") with publishers for campaigns that you co-design? If yes, consider joint controllership for those joint campaigns.

In summary, per data processing activity type:

- Account creation and management (hardware platform account): likely controller, sometimes joint controller or processor.
- Gameplay monitoring (platform telemetry): controller, joint controller when telemetry is co-used with publishers.
- Behavioural inference (platform-level inferences): likely controller.

6.1.2 Creators, designers and developers

Guidance questions:

- Are you running your own community accounts (forums, newsletters, cosmetic reward programmes) to sustain engagement beyond the initial release? If yes, controller.
- Are you operating player accounts purely on behalf of a publisher (publisher branding, privacy policy, instructions on communications)? If yes, processor for that account layer.
- Are you still operating analytics/monitoring for stability, balancing and content updates strictly under a publisher's instructions? If yes, remain processor, and keep evidencing compliance (logs, audits).
- Are you using long-term telemetry across several releases to inform future designs, difficulty curves, or AI systems? If yes, controller for that R&D/analytics use.
- Do you use long-term player histories to build models for new DLC, seasonal passes, or monetisation adjustments across titles? If yes, controller for that profiling.
- Are you only implementing or hosting profiling logic specified and owned by the publisher, without cross-client reuse? If yes, processor for that profiling pipeline.

In summary, per data processing activity type:

- Account creation and management (game accounts): controller for own accounts; processor if accounts are managed for a publisher.
- Gameplay monitoring (game telemetry): processor when collecting telemetry solely for the publisher, controller when using data for own R&D across projects.
- Behavioural inference (game-level inferences): controller when building models for own purposes, processor when building models solely for publisher under instructions.

6.1.3 Development technology providers

Guidance questions:

- Do you keep developer/publisher admin accounts and perhaps player-facing SSO accounts active for long-term analytics, billing, or cross-title features? If yes, controller.
- Where a client uses your identity management service just as a service, and you commit not to reuse data beyond technical security, are you acting under their instructions? If yes, processor for that part.
- Do you keep receiving telemetry from live games over months/years to improve your service, anti-cheat, or engine optimisation? If yes, controller for that continued processing.
- Do you continue to host telemetry solely for one client, under their instructions and without reuse, after launch? If yes, processor obligations (security, deletion, assistance) remain ongoing.
- Are your monetisation/engagement optimisation services trained on data from many titles and used as generic products (e.g., SDK that suggests best timing for offers)? If yes, controller for that profiling.
- Do you and specific clients co-design segmentation and targeting rules in your system (e.g., joint campaigns)? If yes, assess joint controllership.

In summary, per data processing activity type:

- Account creation and management (own service accounts): controller, processor if purely authenticating for a client.
- Gameplay monitoring (service telemetry): often controller, sometimes joint controller; may be processor if truly instruction-bound.
- Behavioural inference (service-level inferences): controller for generic behavioural models (possible joint controller), sometimes processor.

6.1.4 Publishers

Guidance questions:

- Do you keep publisher-wide accounts active for sequels, DLC, seasonal events, and cross-title marketing (email, in-game inbox, push)? If yes, controller, with ongoing obligations.
- Are there co-branded loyalty or membership programmes where you and a platform or store share decision-making on perks and data use? If yes, assess joint controllership for those programmes.
- Are you running LiveOps analytics to monitor engagement, DLC uptake, churn, and monetisation indefinitely or for many years? If yes, controller, with long-term accountability for necessity and minimisation.

- Do you rely on third-party analytics or marketing platforms for ongoing dashboards and campaigns? If they work strictly under your instructions, they are processors; if they reuse aggregated data for their own business, they are at least separate controllers for that reuse.

- Are you maintaining detailed profiles (spend, playtime, modes, response to offers) to run ongoing marketing and in-game personalisation across years? If yes, controller.

In summary, per data protection activity type:

- Account creation and management (publisher accounts): controller, sometimes joint controller with creators, designer and developers.

- Gameplay monitoring (publisher telemetry): controller for telemetry, joint controller with other actors where they co-decide.

- Behavioural inferences (publisher-level inferences): controller for gameplay-based profiling, sometimes joint controller with hardware suppliers/development technology providers/ storefronts.

6.1.5 Storefronts

Guidance questions:

- Are store/launcher accounts used to run long-term wish lists, backlogs, reminders and “come back” campaigns across many titles? If yes, controller.

- Are you co-running recurring events (publisher festivals, franchise spotlights) with shared membership lists? If yes, examine joint controllership for those specific programmes.

- Are you using long-term store/launcher telemetry (installs, playtime, purchase funnel metrics) for A/B tests and merchandising strategies over years? If yes, controller.

- Are some analytics programmes specified together with publishers (e.g., recurring events based on store-wide patterns)? If yes, consider whether that particular programme involves joint controllership.

- Are you profiling players’ long-term purchases, wish list behaviour, and playtime to curate sales, events, and cross-promotions? If yes, controller for that profiling.

- Do you operate joint promotional programmes with publishers that rely on your profiles and their insights (shared targeting rules)? If yes, assess joint controllership for those campaigns.

In summary, per data processing activity type:

- Account creation and management (storefront account): controller, potentially joint controller with publishers for co-branded programs.

- Gameplay monitoring (storefront telemetry): controller for telemetry used to run and optimise the store/launcher, joint controller if co-deciding on telemetry with publishers.

- Behavioural inference (storefront-level inferences): controller for own recommendation and ad-targeting systems, sometimes joint controller with publishers for joint campaigns.

6.2 Managing ongoing operations after launch

6.2.1 Avoiding purpose creep

Live games are not static products. They are always changing: a new matchmaking system is added, a seasonal event changes player behaviour, a guild system grows into a bigger social platform, retention teams ask for more detailed data, designers come up with new reward systems, and safety teams make moderation tools better. Every change may affect the processing of players' personal data.

Purpose creep, the gradual expansion of data use beyond its original scope, is a common risk in the gaming ecosystem where data accumulates and is generated constantly and where commercial incentives are ever present and continuously evolving. This occurs when data collected for one use is repurposed for another that is incompatible with the initial motivation. Even small shifts in how telemetry is interpreted, or who can access it, can alter the nature and scope of processing over time. This can eventually result in different actors processing data for purposes not disclosed to players, violating Article 5(1)(b) GDPR.

This phenomenon is especially common when commercial pressures grow. Data collected for debugging may later become an attractive asset for personalised offers or dynamic pricing. Similarly, behavioural signals gathered for safety may seem useful for engagement prediction or churn modelling. The fact that these uses are tempting or even beneficial to stakeholders does not make them lawful. The controller must reassess if the new use is compatible with the original purpose under Article 6(4).

Purpose creep can also be subtle. Consider a game that collects skill indicators to help with fair matchmaking. Over time, the analytics team may find correlations between skill metrics and the likelihood of purchasing cosmetic items. If these metrics are then used to tailor storefronts or time promotions, gameplay data is repurposed for monetisation in a way players could not expect.

Controllers should conduct structured, periodic reviews of each data processing activity to confirm data use is consistent with the original purpose. If not, controllers must resolve the discrepancy by either limiting processing or establishing a new legal basis and provide the player with updated information.

Consent refresh campaigns are good practice too because the original consent conditions often change substantially, undermining the "specific" and "informed" nature of consent if it is not revisited. Player expectations and contexts also evolve (children becoming adults, changes in play style, sensitivity to tracking, etc.), so periodic reconfirmation helps preserve fairness and alignment with user expectations. From a governance perspective, structured re-permissioning campaigns force controllers to audit purposes, legal bases, and consent records, to clean "orphaned" or undocumented consents, and to improve logs, which helps avoid function creep and strengthens accountability.

6.2.2 Governing the personal data lifecycle

Modern games generate massive datasets. Errors, crashes, movement sequences, economy interactions, chat logs, progression histories, and social interactions accumulate rapidly. If left unchecked,

these datasets grow beyond what is necessary, proportionate, or safe. The principle of data minimisation (Article 5(1)(c) GDPR) requires controllers to process only what is necessary. The principle of storage limitation (Article 5(1)(e) GDPR) states that personal data must not be kept longer than needed.

In practice, data minimisation is not a one-time commitment. It is a long-term process. A retention plan made early on can become obsolete as new features are added or changed. A chat system may need longer retention for initial safety moderation. Later, when it stabilises, long-term logs may no longer be necessary. A telemetry field used during launch-month for balancing may become irrelevant later. Controllers must treat retention as a living process. Inactive accounts should be archived or purged periodically. Logs should be rotated out regularly. Telemetry fields should be assessed and retired as needed. Archives should be anonymised as much as possible once operational needs have passed.

Moreover, the different actors participating in the ecosystem should ensure minimisation is applied consistently across production and testing environments by regularly identifying and deleting datasets that are no longer required. Test environments often accumulate obsolete data, especially when builds change quickly. These forgotten datasets are often the weakest link in a controller's data hygiene and, if not properly managed, can become vectors for breaches.

True minimisation requires confronting the cultural tendency, especially within engineering and analytics teams, to "keep data just in case". To address this, always ensure retained data supports a documented, lawful, and explicit purpose under GDPR. Regularly review and shrink data schemas by removing unnecessary items and fields; this practice directly supports ongoing compliance.

Before adding telemetry events or behavioural inferences to patches or DLC, creators, designers, and developers must: (1) ensure controllers are informed and provide agreement, and (2) update relevant notices to reflect these changes. Development technology providers should provide their clients with a deactivation feature that can be easily triggered remotely in production if an audit reveals a legal or security issue with their service.

6.2.3 Continuous monitoring of data flows and risks

The GDPR's accountability principle under Article 5(2), as well as Articles 24 and 30, obligates controllers to actively map and document personal data flows. Specifically, controllers should identify which teams access each data set, how often, and for what purposes, and keep this documentation up to date to ensure compliance.

Live games often undergo structural changes that subtly alter data pathways. When migrating to a new server region, introducing a new anti-cheat module, or integrating a third-party analytics tool, assess impacts on international transfers, identify new processors, and review retention practices. Always monitor and document these changes as they occur.

Risk assessments and DPIAs should not be reserved solely for major reworks or new features. Instead, they should accompany any change that affects data flow, especially when it involves children's data or behavioural profiling. They are also important for systems that may have significant consequences for players. Regular audits help identify unnecessary data collection, excessive retention, or outdated documented purposes.

6.2.4 Enabling security in a live environment

Another central principle of the GDPR is that of integrity and confidentiality (Article 5(1)(f) GDPR). According to this principle, personal data should be processed in a way that ensures appropriate levels of security against, for example, unauthorised access. The obligation on controllers to properly secure personal data is further defined by Article 32. It cannot be fulfilled solely by the initial technical design and must be seen as an ongoing and continuous obligation. Live games attract adversarial behaviour and threats such as account takeovers, bot networks, cheating rings, credit card fraud, credential stuffing attacks, and attempts to extract high-value in-game items. The security posture of a game must therefore evolve over time to keep up with current challenges. It is recommended to decouple important security updates fixing critical vulnerabilities from conventional functional updates adding new features to the game.

Operational security measures should include: (1) continuous monitoring for anomalous behaviour (from both, people and code elements, specifically, external elements integrated into the game); (2) routine access rights reviews (again from both, people and code elements); (3) vulnerability scanning and internal pen-testing or red-teaming exercises; and (4) periodic code audits. Additionally, encryption keys must be rotated when specific triggering events occur, communication with servers needs to be properly protected, and multi-factor authentication must be made mandatory for both staff and flagged accounts. Controllers are required to document all these measures as part of accountability obligations.

When a breach occurs, Articles 33 and 34 impose strict requirements. The controller must notify the relevant supervisory authority[20] within seventy-two hours after the data controller becomes aware of the breach[21]. If the breach poses a high risk to players, the controller must also inform those affected directly. Clear communication is essential. Players must understand what happened, what data was compromised, and what steps they can take. A breach should never come as a surprise, and it should never be uncovered by players or community forums. Transparency is both a legal requirement and an ethical obligation.

6.3 Promoting mature governance practices

6.3.1. Establishing structures and procedures

The increasing complexity of video games, and online games in particular, requires structured governance around personal data processing. Relying on individual teams to maintain compliance independently often results in fragmented practices and inconsistent protection standards. To meet requirements set out in, among others, Articles 24 and 25, controllers should implement coordinated processes. These include internal privacy committees, cross-disciplinary audits and reviews (such as periodic reviews of automated moderation decisions), and standardised documentation for new processing activities.

[20] EDPB Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82022-identifying-controller-or-processors-lead_en

[21] EDPB Guidelines 9/2022 on personal data breach notification under GDPR, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

Additionally, compliance checks of processors and sub-processors are essential for governance in the video game ecosystem. Controllers rely on a chain of processors and sub-processors (cloud providers, ad-SDKs, analytics firms, etc.) to process personal data. Some recommended practices include pre-onboarding audits. These audits review processor security measures, DPIA inputs, and sub-processor lists before signing DPAs. Other practices are contractual safeguards, such as mandating audit rights, breach notifications, and sub-processor approval or "controller veto". Annual reviews, including incident reports, help maintain protection standards. Aligning with gaming-specific risks, such as avoiding addictive design patterns, is also important. In general, if a decision impacting personal data protection is identified by an actor participating in the ecosystem, they should not make this decision internally but involving the rest of actors in the decision-making process considering their respective GDPR roles and obligations (controller, joint controller, processor, sub-processor).

It should be considered that shared templates for ecosystem actors help build chain-wide compliance. For example, a template for approving any changes in the data processing activity implementation, including when this occurs as part of a maintenance operation.

Finally, organisations should implement and foster a culture of reinforcing literacy on data protection and GDPR compliance through regular and continuous training, adapted to different professional profiles. Developers and live-ops teams need practical training on secure coding, privacy-by-design, and the risks of profiling and automated decision-making in matchmaking, personalisation, and anti-cheat systems. Community managers, marketing, and monetisation teams should receive targeted modules on lawful bases for advertising, consent, and the processing of children's data. Executives and producers should receive high-level briefings on regulatory obligations, DPIA triggers, and data breach-response so that data protection is embedded as a core governance expectation, not an afterthought, across the post-production stage.

6.3.2 Record keeping of processing activities

Article 30 GDPR obliges controllers to maintain records of processing activities. In the dynamic context of video games, these records should serve as an adaptive governance tool, not a static compliance artefact, and must be continuously updated. When a new telemetry field is added, a vendor is onboarded, a retention period is modified, or a feature is retired, records must be promptly revised. Given the iterative nature of game development, with frequent deployments of patches, updates, and transient content, controllers must ensure all changes impacting personal data processing are immediately reflected in their records.

Accurate, current records facilitate compliance with a range of GDPR duties. They enable controllers to respond swiftly and efficiently to data subject requests, perform and update DPIAs, manage data breaches, and defend compliance decisions against regulatory inquiries. Records clarify internal accountability by documenting purposes of processing, categories of personal data, recipients, retention periods, and any transfers to third countries.

As a best practice, companies in the video game industry should embed rigorous record-keeping within product development and management workflows. Doing so enables documentation to proactively reveal and mitigate data protection risks early.

6.3.3 The role of a DPO

The DPO, whether required under Articles 37–39 of the GDPR or appointed voluntarily, plays a critical role in ensuring that data protection considerations are taken into account throughout a game's lifecycle[22]. The DPO must be informed of planned changes that may affect the processing of personal data and should be given the opportunity to provide advice before any final decisions are made. The DPO should thus, among other things, evaluate new features, advise on DPIAs, monitor compliance, audit vendor relationships, and assess risks, particularly those involving high-risk activities such as profiling practices or child participation in social features.

The DPO must act independently and have access to senior leadership. They should be able to raise concerns freely. An organisation should ensure its DPO has sufficient resources and support. The DPO must receive relevant information needed to fulfil their responsibilities effectively. Their participation should be substantive and integrated into governance and decision-making. It should not be limited to formal consultation or mere approval after key decisions have been made. Where the DPO raises concerns about changes to the personal data processing framework, those concerns should be taken seriously and documented.

6.4 End-of-life: legal and technical responsibilities

As a game nears its final phase, data controllers face a heightened period of responsibility and risk, demanding rigorous attention as the title sunsets, regardless of the closure's cause. This end-of-life stage introduces some of the most significant GDPR challenges, notably ensuring fairness, transparency, and careful management of personal data still held by the controller.

Under Articles 12–14 of the GDPR, players should be clearly notified as early as possible about the game's closure. The language used should be unambiguous and hiding messages in marketing materials should be avoided. Controllers should clearly describe what will happen to player accounts, progression, purchases, communications, and in general, all personal data.

When issuing a shutdown notice, controllers should communicate the server closure date, the timeframe for players to request data access or deletion, the types of data to be deleted automatically, and whether anonymised data sets will be kept for research. If migrating players, account migration should be treated as a separate processing activity and players should be informed.

Once processing ends, personal data should be promptly deleted or anonymised in accordance with Article 5(1)(e). Controllers should remove or anonymise all relevant data from production, backups, analytics, and vendor systems, unless they are legally required to retain it. They should keep a written lifecycle policy showing when to stop marketing, anonymise, and delete data at end-of-life.

In removing personal data, controllers can consider the following steps: disable access to the game; clean the underlying databases; anonymise or delete archived data stores; send deletion instructions to all third-party processors. Obtain and save written confirmation for every deletion action.

If retaining data for research, aggregate or process telemetry data in such a way to prevent re-identification. Verify that anonymisation meets the necessary requirements and maintain documentation confirming that re-identification cannot occur.

[22] WP Article 29 Guidelines on Data Protection Officers ("DPOs"), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_en

Annex 1: Checklist for Hardware suppliers (mainly console manufacturers)

Note: This checklist includes game-specific recommendations and good practices included in the previous sections in this document and is not intended to cover all general or well-known GDPR compliance obligations. It should be used as a targeted reference within the video games sector and must be supplemented with a broader legal, organisational and technical review appropriate to your jurisdiction and specific product/service.

Stage	Topic	Description
Pre-production	Accountability	List planned data processing activities and pass the GDPR role gate for each one of them
	Accountability	Document legal basis and purpose (avoiding generic formulation) for each personal data processing activity for which you are controller
	Accountability	Build project checklists, data dictionaries, data lifecycle maps, etc.
	Accountability	Classify behavioural inferences and profiles by potential impact to identify high-risk processing for which a DPIA is necessary and build specific DPIA sections
	Accountability	Provide means and comprehensive documentation to support compliance by other actors
	DPbDD (Data Protection by Design and by Default)	Define minimal platform-level account schema
	DPbDD	Define minimal platform-level telemetry schema

Stage	Topic	Description
Pre-production	DPbDD	Define minimal platform-level behavioural inferences
	DPbDD	Set retention for dev/test platform accounts (early access players), raw telemetry, behavioural profiles, etc. and design/implement enforcement measures such as automated purging or deletion
	DPbDD	Prohibit special category fields in account forms and special category data in telemetry and inferences by default, designing/implementing enforcement measures such as filters
	DPbDD	Chose, encourage and support local data processing
	DPbDD	Design/implement mechanisms for valid parental consent for child testers and early access players
	DPbDD	Offer configuration flags allowing other actors participating in the ecosystem to disable profiling features entirely, for example, in specific regions or for specific accounts
	DPbDD	Optional/monetisation-driven account fields, telemetry and inferences should be turned OFF by default
	DPbDD	Plan optional/monetisation-driven telemetry and inferences opt-out
	DPbDD	Activate parental consent logging for child testers and early access players
	DPbDD	Design/implement age-gates to opt-in risky settings or features (for example, ensure that only accounts marked as “adult” can enable monetisation-oriented profiling)
	DPbDD	Separate safety/functional vs monetisation profiles

Stage	Topic	Description
Pre-production	Rights exercise	Build update/export/delete endpoints for dev/test accounts
	Rights exercise	Tag and document automated decisions
	Rights exercise	Design interface hooks for objection/human review
	Security	Enforce MFA for dev/test account tools
	Security	Use field-level encryption on profile stores
Release	Fairness &Transparency	Clearly distinguish between data strictly necessary for game delivery and data used to optimise monetisation
	Fairness &Transparency	Deploy a dedicated Privacy Centre or Hub
	Fairness &Transparency	Deploy privacy notices citing Article 6 basis per personal data processing activity
	Fairness &Transparency	Rely on privacy labels or similar simplified and visual representations at the point of decision-making
	Fairness &Transparency	Publish platform-level telemetry catalogues, including information on events, fields, recipients, and uses
	Valid consent	Make messages, menus and interfaces legible in different devices and environments
	Valid consent	Block progression until valid consent is captured, rely on layered notices
	Valid consent	Present choices in a granular and balanced way, with separate toggles for categories

Stage	Topic	Description
Release	Valid consent	Keep the player informed proactively using OS notifications, in-app notifications (pop-ups or banners), push alerts, inline warnings and real-time flags, etc.
	Valid consent	Log all interactions concerning consent (timestamp, device ID, choices) in tamper-proof records for auditability
	DPbDD	Lock/prune platform-level account schema
	DPbDD	Lock/prune platform-level telemetry schema
	DPbDD	Lock/prune platform-level behavioural inferences
	DPbDD	Auto-archive platform-level inactive accounts after a fixed period and their associated telemetry and profiles (always with prior notification)
	DPbDD	Default lapsed players re-engagement to maximum privacy settings
	DPbDD	Scan platform-level account forms, telemetry events and behavioural inferences, and reject special category inputs
	DPbDD	Refresh platform-level behavioural profiles at fixed periods (limit platform-level profile windows), and aggregate where possible
	DPbDD	Record every instance where users or devices are categorised into behavioural segments based on telemetry or inferences
	DPbDD	Run verification scripts to guarantee that planned DPbDD measures are deployed properly
	DPbDD	Implement mechanisms for regular platform-level inference models refresh and bias checks

Stage	Topic	Description
Release	Rights exercise	Offer a rights exercise interface embedding this exercise in familiar, game-native interfaces to avoid unnecessary friction
	Rights exercise	Build an always-accessible user interface page where players can view, edit, or opt out of the processing of categories of data tied to their platform-level profiles
	Rights exercise	Deploy a customer support ticketing system
	Rights exercise	Respond to rectification requests without compromising gameplay integrity or opening avenues for abuse
	Rights exercise	Design internal mechanisms to flag and isolate restricted data to prevent inadvertent use in ongoing operations
	Rights exercise	Support and manage an appeal button for automated platform-level account suspensions (with SLA for a maximum review deadline)
	Security	Enforce MFA on all platform-level account recovery flows
	Security	Use unique, game-specific keys for securing personal data transmission from consoles to endpoints in backend servers
Post-production	Accountability	Conduct structured, periodic reviews and audits of each data processing activity to identify unnecessary data collection, excessive retention, outdated purposes, etc.
	Accountability	Monitor and document changes in data processing activities as they occur, ensuring controllers are informed and provide agreement

Stage	Topic	Description
Post-production	Accountability	Update relevant records, documents, notices, etc. regularly to reflect these changes.
	Accountability	Implement/participate in coordinated processes including internal privacy committees, cross-disciplinary audits and reviews, standardised documentation and shared templates, etc.
	Accountability	Conduct periodic compliance checks of processors and sub-processors
	Accountability	Require other actors in the ecosystem, through contractual clauses, to notify games' end-of-life and establish clear responsibilities
	Valid consent	Conduct consent refresh campaigns
	DPbDD	Cease collection of game-specific telemetry at end-of-life and purge stored personal telemetry data (for example, usage stats tied to accounts), anonymise aggregate data for analytics
	DPbDD	Erase or anonymise inferences derived from game behaviour
	Rights exercise	Inform users via console of data options at games' end-of-life, enabling the exercise of their rights
	Rights exercise	Support data deletion or anonymisation requests post end-of-life, providing users clear processes to request removal of personal data such as accounts, telemetry and profiles linked to the game and retaining only anonymised or legally required data
	Security	Decouple important security updates fixing critical vulnerabilities from conventional functional updates

Annex 2: Checklist for Creators, designers and developers

Note: This checklist includes game-specific recommendations and good practices and is not intended to cover all general or well-known GDPR compliance obligations. It should be used as a targeted reference within the video games sector and must be supplemented with a broader legal, organisational and technical review appropriate to your jurisdiction and specific product/service.

Stage	Topic	Description
Pre-production	Accountability	Ensure that different teams treat data protection as a core design requirement, equivalent to gameplay or narrative considerations
	Accountability	List planned data processing activities and pass the GDPR role gate for each one of them
	Accountability	Document legal basis and purpose (avoiding generic formulation) for each personal data processing activity in all those for which you are controller
	Accountability	Build project checklists, data dictionaries, data lifecycle maps, etc.
	Accountability	Classify behavioural inferences and profiles by potential impact to identify high-risk processing and build specific DPIA sections and/or suggest the publisher to conduct a joint DPIA
	Accountability	Provide means and comprehensive documentation to support compliance by other actors
	Accountability	Prepare a “telemetry notice” template for external playtests that explains what is recorded during tests, who sees it, and how long it is recorded during tests (this information must be aligned with publisher’s notices)

Stage	Topic	Description
Pre-production	Accountability	Add a short “Profiling role sheet” per model when scoping AI/personalisation features in preproduction: who owns it, who can reuse it, and whether you are the controller or the processor
	Accountability	Disclose NPC data practices through contextual notices and comprehensive privacy policies that detail flows, retention, and AI involvement
	DPbDD (Data Protection by Design and by Default)	Define minimal game account schema
	DPbDD	Define minimal game telemetry schema
	DPbDD	Tag telemetry events: “studio only”, “publisher only”, “studio reuse” (the latter requires your own legal basis and records of processing
	DPbDD	Define minimal game-level behavioural inferences
	DPbDD	Evaluate game mechanics and progression systems to ensure they do not require disproportionate processing of players’ personal data; if multiple technical options exist, select the least intrusive design that meets gameplay and narrative objectives
	DPbDD	Audit accuracy in AI-driven NPCs processing and bias in their decision-making
	DPbDD	Set retention for dev/test game accounts (early access players), raw telemetry, behavioural profiles, data processed by NPCs, etc. and design/implement enforcement measures such as automated purging or deletion

Stage	Topic	Description
Pre-production	DPbDD	Prohibit special category fields in account forms and special category data in telemetry and inferences by default, designing/implementing enforcement measures such as filters
	DPbDD	Design telemetry and inferences as local-first, flag server uploads, for example, for granular consent
	DPbDD	Specify an age threshold when you recruit minors for early playtests, create separate parental consent forms with verifiable logging, and ensure these records are stored alongside the tester's account ID
	DPbDD	Offer configuration flags allowing other actors participating in the ecosystem to disable game profiling features entirely, for example, in specific regions or for specific accounts
	DPbDD	Default optional/monetisation-driven account fields, telemetry and inferences OFF
	DPbDD	Plan optional/monetisation-driven game telemetry and inferences opt-out
	DPbDD	Embed children safety into the game's design and architecture: implement restricted communication modes, automated filtering, guardian dashboards, spending limits, time-of-day restrictions, accessible reporting tools, etc.
	DPbDD	Design/implement age-gates to opt-in risky settings or features
	DPbDD	Separate safety/functional vs monetisation profiles

Stage	Topic	Description
Pre-production	DPbDD	Conduct UX testing for deceptive and addictive patterns via independent audits
	DPbDD	Rely on synthetic data, when possible, to train AI-driven NPCs, and minimise the training dataset in the rest of the cases, by aggregating or pseudonymising inputs
	Rights exercise	Build update/export/delete endpoints for dev/test accounts
	Rights exercise	Tag and document automated decisions
	Rights exercise	Design interface hooks for objection/human review
	Security	Enforce MFA for dev/test account tools
	Security	Use field-level encryption on profile stores
Release	Fairness &Transparency	Clearly distinguish between data strictly necessary for game delivery and data used to optimise monetisation
	Fairness &Transparency	Deploy a dedicated Privacy Centre or Hub
	Fairness &Transparency	Deploy privacy notices citing Article 6 basis per personal data processing activity
	Fairness &Transparency	Rely on privacy labels or similar simplified and visual representations at the point of decision-making
	Fairness &Transparency	Publish game telemetry catalogues, including information on events, fields, recipients, and uses

Stage	Topic	Description
Release	Fairness &Transparency	Prioritise “runtime permissions” (triggered when a feature like voice chat is actually used) over “install-time permissions”
	Valid consent	Make messages, menus and interfaces legible in different devices and environments
	Valid consent	Block progression until valid consent is captured, rely on layered notices
	Valid consent	Present choices in a granular and balanced way, with separate toggles for categories
	Valid consent	Keep the player informed proactively using in-game notifications (pop-ups or banners), push alerts, inline warnings and real-time flags, etc.
	Valid consent	Log all interactions concerning consent (timestamp, device ID, choices) in tamper-proof records for auditability
	DPbDD	Lock/prune game account schema
	DPbDD	Lock/prune game telemetry schema
	DPbDD	Lock/prune game-level behavioural inferences
	DPbDD	Auto-archive game inactive accounts after a fixed period and their associated telemetry and profiles (always with prior notification)
	DPbDD	Default lapsed players re-engagement to maximum privacy settings

Stage	Topic	Description
Release	DPbDD	Default “stealth mode”, ensure all optional account fields and data sharing with third parties are OFF by default, requiring an explicit opt-in for activation
	DPbDD	Scan game account forms, telemetry events and behavioural inferences, and reject special category inputs
	DPbDD	Refresh game-level behavioural profiles at fixed periods (limit profile windows), and aggregate where possible
	DPbDD	Record every instance where players are categorised into behavioural segments based on telemetry or inferences
	DPbDD	Run verification scripts to guarantee that planned DPbDD measures are deployed properly
	DPbDD	Implement mechanisms for regular game-level inference models refresh and bias checks
	DPbDD	Support players well-being by building in checkpoints, auto-saves, and natural breaks (session timers, “rest suggested” prompts) to curb over-engagement
	Rights exercise	Offer a rights exercise interface embedding this exercise in familiar, game-native interfaces to avoid unnecessary friction
	Rights exercise	Build an always-accessible user interface page where players can view, edit, or opt out of data categories tied to their game-level profiles
	Rights exercise	Deploy a customer support ticketing system
	Rights exercise	Respond to rectification requests without compromising gameplay integrity or opening avenues for abuse

Stage	Topic	Description
Release	Rights exercise	Design internal mechanisms to flag and isolate restricted data to prevent inadvertent use in ongoing operations
	Rights exercise	Support and manage an appeal button for automated game account suspensions (with SLA for a maximum review deadline)
	Security	Enforce MFA on all game account recovery flows
	Security	Deploy role-based access for dev teams
	Security	Use unique, game-specific keys for securing personal data transmission from players' devices to endpoints in backend servers
Post-production	Accountability	Conduct structured, periodic reviews and audits of each data processing activity to identify unnecessary data collection, excessive retention, outdated purposes, etc.
	Accountability	Monitor and document changes in data processing activities as they occur, ensuring controllers are informed and provide agreement
	Accountability	Update relevant records, documents, notices, etc. regularly to reflect these changes
	Accountability	Implement/participate in coordinated processes including internal privacy committees, cross-disciplinary audits and reviews, standardised documentation and shared templates, etc.
	Accountability	Conduct periodic compliance checks of processors and sub-processors

Stage	Topic	Description
Post-production	Accountability	Notify games' end-of-life to other actors participating in the ecosystem and establish clear responsibilities
	Valid consent	Conduct consent refresh campaigns
	DPbDD	Ensure minimisation is applied consistently across production and testing environments by regularly identifying and deleting datasets that are no longer required
	DPbDD	Cease collection of game-specific telemetry at end-of-life and purge stored personal telemetry data, anonymise aggregate data for analytics
	DPbDD	Erase or anonymise inferences derived from game behaviour
	Rights exercise	Inform users of data options at games' end-of-life, enabling the exercise of their rights
	Rights exercise	Support data deletion or anonymisation requests post end-of-life, providing users clear processes to request removal of personal data such as accounts, telemetry and profiles linked to the game and retaining only anonymised or legally required data
	Security	Implement game account anomaly detection mechanisms
	Security	Decouple important security updates fixing critical vulnerabilities from conventional functional updates

Annex 3: Checklist for Development technology providers

Note: This checklist includes game-specific recommendations and good practices included in the previous sections in this document and is not intended to cover all general or well-known GDPR compliance obligations. It should be used as a targeted reference within the video games sector and must be supplemented with a broader legal, organisational and technical review appropriate to your jurisdiction and specific product/service.

Stage	Topic	Description
Pre-production	Accountability	List planned data processing activities and pass the GDPR role gate for each one of them
	Accountability	Document legal basis and purpose (avoiding generic formulation) for each personal data processing activity in all those for which you are controller
	Accountability	Build project checklists, data dictionaries, data lifecycle maps, etc.
	Accountability	Classify behavioural inferences and profiles by potential impact to identify high-risk processing and build specific DPIA sections
	Accountability	Provide template wording so different actors participating in the ecosystem can clearly explain whether they co-control authentication (e.g., “X authenticates your account on our behalf”)
	Accountability	Provide means and comprehensive documentation to support compliance by other actors: a dataflow diagram per product that explicitly lists data fields, recipients, controllership, and configuration options, standard contract clauses, detailed “profiling data sheet” for each behavioural module (including inputs, outputs, purposes, the controller, and how data subjects can exercise their rights), etc.

Stage	Topic	Description
Pre-production	Accountability	Include contractual clauses that forbid clients from passing “known minors” labels into profiling APIs without additional agreed-upon safeguards
	DPbDD (Data Protection by Design and by Default)	Design the service so that functionalities (audience analytics, advertising retargeting, etc.) are decorrelated, allowing clients to select only the modules they need
	DPbDD	Define minimal service account schema
	DPbDD	Separate “tool user” accounts (for dev teams) from “player” accounts
	DPbDD	Define minimal SDK telemetry schema
	DPbDD	Define minimal SDK behavioural inferences
	DPbDD	Set retention for service accounts, raw telemetry, behavioural profiles, etc. and design/implement enforcement measures such as automated purging or deletion
	DPbDD	Prohibit special category fields in account forms and special category data in telemetry and inferences by default, designing/implementing enforcement measures such as filters
	DPbDD	Chose, encourage and support local data processing
	DPbDD	Offer configuration flags allowing other actors participating in the ecosystem to disable profiling features entirely, for example, in specific regions or for specific accounts

Stage	Topic	Description
Pre-production	DPbDD	Expose granular toggles for data sync, opt-ins, etc.
	DPbDD	Ensure SDK dashboards display only aggregated metrics, accessing raw, player-level telemetry must require a time-bound, logged privilege escalation process
	DPbDD	Design your tools to accept and process an age signal so that features can be restricted/enabled automatically depending on the assured age
	DPbDD	Default optional/monetisation-driven account fields, telemetry and inferences OFF
	DPbDD	Plan optional/monetisation-driven telemetry and inferences opt-out
	DPbDD	Separate safety/functional vs monetisation profiles
	DPbDD	Conduct UX testing for deceptive and addictive patterns via independent audits
	Rights exercise	Tag and document automated decisions
	Rights exercise	Design interface hooks for objection/human review
	Security	Enforce logical separation, implementing per-client keys or database schemas to avoid cross-tenant access by design
	Security	Encrypt service payloads end-to-end
	Security	Use field-level encryption on profile stores

Stage	Topic	Description
Release	Fairness &Transparency	Clearly distinguish between data strictly necessary for service delivery and data used to optimise monetisation
	Fairness &Transparency	Deploy a dedicated Privacy Centre or Hub, including a dashboard for live transparency (for example, “Profile used X times this week”)
	Fairness &Transparency	Deploy privacy notices citing Article 6 basis per personal data processing activity
	Fairness &Transparency	Rely on privacy labels or similar simplified and visual representations at the point of decision-making
	Fairness &Transparency	Publish SDK telemetry catalogues, including information on events, fields, recipients, and uses
	Valid consent	Make messages, menus and interfaces legible in different devices and environments
	Valid consent	Present choices in a granular and balanced way, with separate toggles for categories
	Valid consent	Design your service to allow its execution to be suspended until the host application sends a signal that valid consent has been obtained
	Valid consent	Log all interactions concerning consent (timestamp, device ID, choices) in tamper-proof records for auditability
	DPbDD	Lock/prune service account schema
	DPbDD	Lock/prune SDK telemetry schema

Stage	Topic	Description
Release	DPbDD	Lock/prune SDK behavioural inferences
	DPbDD	Auto-archive service inactive accounts after a fixed period and their associated telemetry and profiles (always with prior notification)
	DPbDD	Scan service account forms, telemetry events and behavioural inferences, and reject special category inputs
	DPbDD	Refresh SDK behavioural profiles at fixed periods (limit platform-level profile windows), and aggregate where possible
	DPbDD	Record every instance where users or devices are categorised into behavioural segments based on telemetry or inferences
	DPbDD	Run verification scripts to guarantee that planned DPbDD measures are deployed properly
	DPbDD	Implement mechanisms for regular SDK inference models refresh and bias checks
	DPbDD	Auto-disable inactive service features
	Rights exercise	Provide APIs that allow clients to automatically reflect player requests (access, portability, or deletion) across your technical infrastructure
	Rights exercise	Offer a rights exercise interface embedding this exercise in familiar, easy-to-use interfaces to avoid unnecessary friction
	Rights exercise	Deploy a customer support ticketing system

Stage	Topic	Description
Release	Rights exercise	Respond to rectification requests without compromising gameplay integrity or opening avenues for abuse
	Rights exercise	Design internal mechanisms to flag and isolate restricted data to prevent inadvertent use in ongoing operations
	Security	Notify anomalies to clients (for example, unusual profiling spikes)
	Security	Enforce MFA on all service account recovery flows
Post-production	Accountability	Conduct structured, periodic reviews and audits of each data processing activity to identify unnecessary data collection, excessive retention, outdated purposes, etc.
	Accountability	Monitor and document changes in data processing activities as they occur, ensuring controllers are informed and provide agreement
	Accountability	Update relevant records, documents, notices, etc. regularly to reflect these changes.
	Accountability	Implement/participate in coordinated processes including internal privacy committees, cross-disciplinary audits and reviews, standardised documentation and shared templates, etc.
	Accountability	Conduct periodic compliance checks of processors and sub-processors
	Accountability	Require other actors in the ecosystem, through contractual clauses, to notify games' end-of-life and establish clear responsibilities

Stage	Topic	Description
Post-production	Valid consent	Ensure that the revocation of a player's consent does not lead to game instability or cause your service to constantly re-request permissions
	Valid consent	Conduct consent refresh campaigns
	DPbDD	Cease collection of game-specific telemetry at end-of-life and purge stored personal telemetry data (for example, usage stats tied to accounts), anonymise aggregate data for analytics if no longer linked to individuals
	DPbDD	Erase or anonymise inferences derived from game behaviour
	DPbDD	Regularly update your software to benefit from the latest, more privacy-friendly OS and hardware-platform APIs
	DPbDD	Provide clients with a deactivation feature that can be easily triggered remotely in production if an audit reveals a legal or security issue with your software
	Rights exercise	Support data deletion or anonymisation requests post end-of-life, providing users clear processes to request removal of personal data such as accounts, telemetry and profiles linked to the game and retaining only anonymised or legally required data
	Security	Decouple important security updates fixing critical vulnerabilities from conventional functional updates

Annex 4: Checklist for Publishers

Note: This checklist includes game-specific recommendations and good practices and is not intended to cover all general or well-known GDPR compliance obligations. It should be used as a targeted reference within the video games sector and must be supplemented with a broader legal, organisational and technical review appropriate to your jurisdiction and specific product/service.

Stage	Topic	Description
Pre-production	Accountability	List planned data processing activities and pass the GDPR role gate for each one of them
	Accountability	Document legal basis and purpose (avoiding generic formulation) for each personal data processing activity in all those for which you are controller
	Accountability	Build project checklists, data dictionaries, data lifecycle maps, etc.
	Accountability	Classify behavioural inferences and profiles by potential impact to identify high-risk processing and build specific DPIA sections and/or suggest other actors to conduct a joint DPIA
	Accountability	Provide means and comprehensive documentation to support compliance by other actors
	Accountability	Prepare a “telemetry notice” template for external playtests that explains what is recorded during tests, who sees it, and how long it is recorded during tests
	Accountability	Add a short “Profiling role sheet” per model when scoping AI/personalisation features in preproduction: who owns it, who can reuse it, and whether you are the controller or the processor

Stage	Topic	Description
Pre-production	DPbDD	Define minimal publisher account schema. Determine early whether accounts will be per-game or shared; if shared, constrain default data fields to the minimum intersection needed for all titles rather than a broad superset.
	DPbDD	Keep a separate registry entry for alpha/beta signups, recording what data are collected (emails, age, platform IDs) and whether they will later be used for marketing or future titles.
	DPbDD	Define minimal publisher telemetry schema
	DPbDD	Plan how player's data or profile will be linked across multiple games and make this linking optional
	DPbDD	Tag telemetry events: "studio only", "publisher only", "studio reuse", etc.
	DPbDD	Define minimal publisher-level behavioural inferences
	DPbDD	Set retention for publisher accounts (early access players), raw telemetry, behavioural profiles, etc. and design/implement enforcement measures such as automated purging or deletion
	DPbDD	Prohibit special category fields in account forms and special category data in telemetry and inferences by default, designing/implementing enforcement measures such as filters
	DPbDD	Use synthetic or strongly anonymised test data by default; avoid real player data in development and pre-production environments.

Stage	Topic	Description
Pre-production	DPbDD	Design telemetry and inferences as local-first, flag server uploads, for example, for granular consent
	DPbDD	Specify an age threshold when you recruit minors for different initiatives and tests, create separate parental consent forms with verifiable logging, and ensure these records are stored alongside the tester's account ID
	DPbDD	If the publisher provides many different services, allow the player to independently use each of the services offered
	DPbDD	Default optional/monetisation-driven account fields, telemetry and inferences OFF
	DPbDD	Plan optional/monetisation-driven publisher telemetry and inferences opt-out
	DPbDD	Design/implement age-gates to opt-in risky settings or features
	DPbDD	Separate safety/functional vs monetisation profiles
	DPbDD	Conduct UX testing for deceptive and addictive patterns via independent audits and explicitly incentivise creators, designers and developers not to use these patterns.
	DPbDD	Minimise the data transmitted to business partners and third-party providers, transmitting identifying data (name, alias or nickname, unique identifier number, etc.) only when strictly necessary
	Rights exercise	Build update/export/delete endpoints for publisher accounts

Stage	Topic	Description
Pre-production	Rights exercise	Specify in alpha/beta agreements with testers whether telemetry is anonymised/aggregated and whether it will feed future titles or profiling, adjusting transparency and choice mechanisms accordingly
	Rights exercise	Tag and document automated decisions
	Rights exercise	Design interface hooks for objection/human review
	Security	Secure accounts with strong password storage, MFA where appropriate (for example, administrative users), session protection, rate limiting, and abuse detection
	Security	Use field-level encryption on profile stores
Release	Fairness &Transparency	Clearly distinguish between data strictly necessary for games delivery and data used to optimise monetisation
	Fairness &Transparency	Inform players about the transmission of their personal data to business partners and third-party providers
	Fairness &Transparency	Deploy a dedicated Privacy Centre or Hub
	Fairness &Transparency	Deploy privacy notices citing Article 6 basis per personal data processing activity
	Fairness &Transparency	Rely on privacy labels or similar simplified and visual representations at the point of decision-making
	Fairness &Transparency	Publish publisher telemetry catalogues, including information on events, fields, recipients, and uses

Stage	Topic	Description
Release	Valid consent	Make messages, menus and interfaces legible in different devices and environments
	Valid consent	Present choices in a granular and balanced way, with separate toggles for categories and avoiding “bundled” consent (for example, ensure that consent for marketing is distinct from the acceptance of the Terms of Service)
	Valid consent	Log all interactions concerning consent (timestamp, device ID, choices) in tamper-proof records for auditability
	DPbDD	Lock/prune publisher account schema
	DPbDD	Lock/prune publisher telemetry schema
	DPbDD	Lock/prune publisher-level behavioural inferences
	DPbDD	Auto-archive inactive accounts after a fixed period and their associated telemetry and profiles (always with prior notification)
	DPbDD	Default “stealth mode”, ensure all optional account fields and data sharing with third parties are OFF by default, requiring an explicit opt-in for activation
	DPbDD	Scan publisher account forms, telemetry events and behavioural inferences, and reject special category inputs
	DPbDD	Refresh publisher-level behavioural profiles at fixed periods (limit profile windows), and aggregate where possible
	DPbDD	Record every instance where players are categorised into behavioural segments based on telemetry or inferences

Stage	Topic	Description
Release	DPbDD	Run verification scripts to guarantee that planned DPbDD measures are deployed properly
	DPbDD	Implement mechanisms for regular publisher-level inference models refresh and bias checks
	Rights exercise	Offer a rights exercise interface embedding this exercise in familiar, game-native interfaces to avoid unnecessary friction and providing a unique tool to access, correct, or delete their data across multiple titles
	Rights exercise	Build an always-accessible user interface page where players can view, edit, export (when possible) or opt out of data categories tied to their publisher-level profiles
	Rights exercise	Identify portable data and facilitate exports via coordination supported by contracts (ensure storefronts or developers to propagate requests across the stack, etc.)
	Rights exercise	Deploy a central opt-out function blocking telemetry or behavioural inferences across all titles, with opt-out options persisting across reinstalls
	Rights exercise	Deploy a customer support ticketing system
	Rights exercise	Design internal mechanisms to flag and isolate restricted data to prevent inadvertent use in ongoing operations
	Rights exercise	Provide players with explanations of why they were targeted with a specific mechanic or offer
	Rights exercise	Design a centralised, internal tool that allows tracking and managing all in-game sanctions (bans, suspensions, etc.) and their associated player appeals across the entire portfolio of titles (not just one game at a time)

Stage	Topic	Description
Release	Security	Clearly separate database systems (or at least schemas and access controls) for core game/service data (accounts, progression, payments, matchmaking, etc.), and marketing/CRM/analytics data (email lists, campaign tracking, attribution data, etc.)
Post-production	Accountability	Conduct structured, periodic reviews and audits of each data processing activity to identify unnecessary data collection, excessive retention, outdated purposes, etc.
	Accountability	Set up a validation process to approve any changes in the conditions for implementing the processing including when this occurs as part of a game maintenance operation
	Accountability	Monitor and document changes in data processing activities as they occur, ensuring controllers are informed and provide agreement
	Accountability	Update relevant records, documents, notices, etc. regularly to reflect these changes
	Accountability	Implement/participate in coordinated processes including internal privacy committees, cross-disciplinary audits and reviews, standardised documentation and shared templates, etc.
	Accountability	Conduct periodic compliance checks of processors and sub-processors
	Valid consent	Conduct consent refresh campaigns
	DPbDD	Reassess whether all telemetry streams and inferences are still necessary after launch, and delete any that no longer serve a documented purpose

Stage	Topic	Description
Post-production	DPbDD	Cease collection of game-specific telemetry at end-of-life and purge stored personal telemetry data, anonymise aggregate data for analytics if no longer linked to individuals
	DPbDD	Erase or anonymise inferences derived from game behaviour
	Rights exercise	Inform users of data options at games' end-of-life, enabling the exercise of their rights
	Rights exercise	Support data deletion or anonymisation requests post end-of-life, providing users clear processes to request removal of personal data such as accounts, telemetry and profiles linked to the game and retaining only anonymised or legally required data
	Security	Implement account anomaly detection mechanisms
	Security	Keep incident response playbooks for account compromise, telemetry or inferences breaches and accidental exposure of test systems

Annex 5: Checklist for Storefronts

Note: This checklist includes game-specific recommendations and good practices and is not intended to cover all general or well-known GDPR compliance obligations. It should be used as a targeted reference within the video games sector and must be supplemented with a broader legal, organisational and technical review appropriate to your jurisdiction and specific product/service.

Stage	Topic	Description
Pre-production	Accountability	List planned data processing activities and pass the GDPR role gate for each one of them
	Accountability	Document legal basis and purpose (avoiding generic formulation) for each personal data processing activity in all those for which you are controller
	Accountability	Build project checklists, data dictionaries, data lifecycle maps, etc.
	Accountability	Provide means and comprehensive documentation to support compliance by other actors (for example, a “role one pager” for each alpha/beta programme to publishers, so both sides can align privacy notices or DPIAs)
	Accountability	When setting up alpha/beta programmes through the store, clarify in contracts which consents/notices the store shows, what data the publisher receives, and under which role (independent controller vs processor)
	Accountability	Prepare a “telemetry notice” template for external playtests that explains what is recorded during tests, who sees it, and how long it is recorded during tests
	Accountability	Add a short “Profiling role sheet” per model when scoping AI/personalisation features in preproduction: who owns it, who can reuse it, specific data sources, and whether you are the controller or the processor

Stage	Topic	Description
Pre-production	DPbDD (Data Protection by Design and by Default)	Define minimal storefront account schema. Determine early whether accounts will be per-game or shared; if shared, constrain default data fields to the minimum intersection needed for all titles rather than a broad superset.
	DPbDD	Keep a separate registry entry for alpha/beta signups, recording what data are collected (emails, age, platform IDs) and whether they will later be used for marketing or other purposes.
	DPbDD	Define minimal storefront telemetry schema
	DPbDD	Plan how player's data or profile will be linked across multiple games and make this linking (and cross-promotion based on it) optional
	DPbDD	Tag telemetry events ("publisher only", "storefront only", etc.) Clearly distinguishing store analytics from per game analytics
	DPbDD	Define minimal storefront-level behavioural inferences
	DPbDD	Set retention for storefront accounts (early access players), raw telemetry, behavioural profiles, etc. and design/implement enforcement measures such as automated purging or deletion
	DPbDD	Prohibit special category fields in account forms and special category data in telemetry and inferences by default, designing/implementing enforcement measures such as filters
	DPbDD	Use synthetic or strongly anonymised test data by default; avoid real player data in development and pre-production environments.

Stage	Topic	Description
Pre-production	DPbDD	Design telemetry and inferences as local-first, flag server uploads, for example, for granular consent
	DPbDD	Specify an age threshold when you recruit minors for different initiatives and tests, create separate parental consent forms with verifiable logging, and ensure these records are stored alongside the tester's account ID
	DPbDD	Default optional/monetisation-driven account fields, telemetry and inferences OFF
	DPbDD	Plan optional/monetisation-driven storefront telemetry and inferences opt-out
	DPbDD	Design/implement age-gates to opt-in risky settings or features (social functions, personalised marketing, etc.)
	DPbDD	Separate safety/functional vs monetisation profiles
	DPbDD	Conduct UX testing for deceptive and addictive patterns via independent audits and explicitly incentivise other actors not to use these patterns.
	DPbDD	Minimise the data transmitted to business partners and third-party providers, transmitting identifying data (name, alias or nickname, unique identifier number, etc.) only when strictly necessary, use narrowly scoped tokens rather than full account records
	Rights exercise	Build update/export/delete endpoints for storefront accounts

Stage	Topic	Description
Pre-production	Rights exercise	Specify in alpha/beta agreements with testers whether telemetry is anonymised/aggregated and whether it will feed future titles or profiling, adjusting transparency and choice mechanisms accordingly
	Rights exercise	Tag and document automated decisions
	Rights exercise	Design interface hooks for objection/human review
	Security	Secure accounts with strong password storage, MFA where appropriate (for example, administrative users), session protection, rate limiting, and abuse detection
	Security	Use field-level encryption on profile stores
Release	Fairness &Transparency	Ensure all privacy-related information and PEGI age ratings are available to the user before the purchase or download button is clicked
	Fairness &Transparency	Clearly distinguish between data strictly necessary for games delivery and data used to optimise monetisation
	Fairness &Transparency	Provide privacy filters in your search options so players can find games with/without specific data processing practices
	Fairness &Transparency	Inform players about the transmission of their personal data to business partners and third-party providers
	Fairness &Transparency	Deploy a dedicated Privacy Centre or Hub
	Fairness &Transparency	Deploy privacy notices citing Article 6 basis per personal data processing activity

Stage	Topic	Description
Release	Fairness &Transparency	Rely on privacy labels or similar simplified and visual representations at the point of decision-making
	Fairness &Transparency	Publish storefront telemetry catalogues, including information on events, fields, recipients, and uses
	Fairness &Transparency	Provide clear reporting tools within the launcher so players can flag different threats, such as harmful content or deceptive&addictive design in games
	Valid consent	Make messages, menus and interfaces legible in different devices and environments
	Valid consent	Present choices in a granular and balanced way, with separate toggles for categories and avoiding “bundled” consent (for example, ensure that consent for marketing is distinct from the acceptance of the Terms of Service)
	Valid consent	Log all interactions concerning consent (timestamp, device ID, choices) in tamper-proof records for auditability
	DPbDD	Lock/prune storefront account schema
	DPbDD	Lock/prune storefront telemetry schema
	DPbDD	Lock/prune storefront-level behavioural inferences
	DPbDD	Auto-archive inactive accounts after a fixed period and their associated telemetry and profiles (always with prior notification)
	DPbDD	Default “stealth mode”, ensure all optional account fields and data sharing with third parties are OFF by default, requiring an explicit opt-in for activation

Stage	Topic	Description
Release	DPbDD	Scan storefront account forms, telemetry events and behavioural inferences, and reject special category inputs
	DPbDD	Refresh storefront-level behavioural profiles at fixed periods (limit profile windows), and aggregate where possible
	DPbDD	Record every instance where players are categorised into behavioural segments based on telemetry or inferences
	DPbDD	Run verification scripts to guarantee that planned DPbDD measures are deployed properly
	DPbDD	Implement mechanisms for regular storefront-level inference models refresh and bias checks
	Rights exercise	Offer a rights exercise interface embedding this exercise in familiar, game-native interfaces to avoid unnecessary friction and providing a unique tool to access, correct, or delete their data across multiple titles
	Rights exercise	Build an always-accessible user interface page where players can view, edit, export (when possible) or opt out of data categories tied to their storefront-level profiles
	Rights exercise	Identify portable data and facilitate exports via coordination supported by contracts
	Rights exercise	Deploy a central opt-out function blocking telemetry or behavioural inferences across all titles, with opt-out options persisting across reinstalls
	Rights exercise	Deploy a customer support ticketing system

Stage	Topic	Description
Release	Rights exercise	Design internal mechanisms to flag and isolate restricted data to prevent inadvertent use in ongoing operations
	Rights exercise	Provide players with explanations of why they were targeted with a specific offer
	Rights exercise	Design a centralised, internal tool that allows tracking and managing all in-game sanctions (bans, suspensions, etc.) and their associated player appeals across the entire portfolio of titles (not just one game at a time)
	Security	Clearly separate database systems (or at least schemas and access controls) for core game/service data (accounts, progression, payments, matchmaking, etc.), and marketing/CRM/analytics data (email lists, campaign tracking, attribution data, etc.)
Post-production	Accountability	Conduct structured, periodic reviews and audits of each data processing activity to identify unnecessary data collection, excessive retention, outdated purposes, etc.
	Accountability	Set up a validation process to approve any changes in the conditions for implementing the processing including when this occurs as part of an update or maintenance operation
	Accountability	Monitor and document changes in data processing activities as they occur, ensuring controllers are informed and provide agreement
	Accountability	Update relevant records, documents, notices, etc. regularly to reflect these changes

Stage	Topic	Description
Post-production	Accountability	Implement/participate in coordinated processes including internal privacy committees, cross-disciplinary audits and reviews, standardised documentation and shared templates, etc.
	Accountability	Conduct periodic compliance checks of processors and sub-processors
	Valid consent	Conduct consent refresh campaigns
	DPbDD	Reassess whether all telemetry streams and inferences are still necessary after launch, and delete any that no longer serve a documented purpose
	DPbDD	Cease collection of game-specific telemetry at end-of-life and purge stored personal telemetry data, anonymise aggregate data for analytics if no longer linked to individuals
	DPbDD	Erase or anonymise inferences derived from game behaviour
	Rights exercise	Inform users of data options at games' end-of-life, enabling the exercise of their rights
	Rights exercise	Support data deletion or anonymisation requests post end-of-life, providing users clear processes to request removal of personal data such as accounts, telemetry and profiles linked to the game and retaining only anonymised or legally required data
	Security	Implement account anomaly detection mechanisms
	Security	Keep incident response playbooks for account compromise, telemetry leakage, and accidental exposure in inferences or test systems


aepd
agencia
española
protección
datos


Autorité de protection des données
Gegevensbeschermingsautoriteit