# A Decision-Support Framework for GDPR Compliance and Data Protection Impact Assessment in Serious Games Validation

Rana Saniei
Computer Engineering Faculty
Universidad Complutense de Madrid
Madrid, Spain
rsaniei@ucm.es

Cristina Alonso-Fernández
Computer Engineering Faculty
Universidad Complutense de Madrid
Madrid, Spain
calonsofernandez@ucm.es

Antonio Calvo-Morata
Computer Engineering Faculty
Universidad Complutense de Madrid
Madrid, Spain
antcal01@ucm.es

Baltasar Fernández-Manjón
Computer Engineering Faculty
Universidad Complutense de Madrid
Madrid, Spain
balta@fdi.ucm.es

***Abstract*—Serious game validation increasingly relies on the collection and analysis of diverse types of personal data, ranging from questionnaires and gameplay logs to behavioural and physiological information. While data protection regulations such as the General Data Protection Regulation (GDPR) establish important legal requirements, translating these requirements into practical decisions during the design of validation studies remains challenging for researchers. This paper presents a decision-support framework that helps serious game researchers identify relevant data protection obligations during the planning of validation activities. The framework combines GDPR requirements, WP29 Data Protection Impact Assessment (DPIA) guidelines, and domain-specific recommendations to guide researchers through a structured description of their validation process. Based on the characteristics of the planned study, the framework identifies potentially high-risk processing activities and generates tailored compliance recommendations. The proposed approach aims to facilitate privacy-by-design practices, improve consistency in compliance assessment, and reduce the need for specialised legal expertise during serious game validation.**

***Index Terms*—Serious Games Validation, GDPR, Privacy by Design (PbD), Decision-Support Systems**

## I. Introduction

Modern serious games (SGs) increasingly function as data-intensive experimental environments rather than simple interactive applications. They are widely used in domains such as education, healthcare, and training, where they provide interactive environments for learning and behavioral change [9]. In these contexts, serious games generate and collect diverse types of data both during gameplay and throughout their validation processes. Validation commonly includes mechanisms such as questionnaires (pre- and post-tests), interviews, log-based data collection, oral discussions, video recordings, and observational analysis [6]. These approaches may be combined to capture different perspectives on player experience and learning outcomes.

Across these processes, a wide range of data is collected, including demographic information, test scores, player feedback, in-game behavioral data (telemetry), and physiological or sensor-based signals such as heart rate, skin conductance, eye tracking, and facial expressions [5]. Researchers may also rely on advanced technologies such as AR/VR systems, behavioral monitoring tools, and AI-based analytics to support both data collection and analysis. Learning analytics and machine learning techniques are frequently applied to extract insights from these datasets for different stakeholders [11], including game designers aiming to improve game quality and educators who use the results to monitor learners performance. More recently, Generative AI has also been explored as a means of deriving additional insights from complex multimodal datasets [21].

An important application of this data is the serious game validation process itself, which has become increasingly complex due to multimodal data collection, advanced analytics, and the involvement of diverse user groups, including minors and other vulnerable populations. As a result, in the validation of serious games, evaluation is not limited to usability and effectiveness, but also increasingly includes legal, ethical, and data protection considerations related to data collection. [19] introduces additional complexity, as serious games rely on multi-layered datasets that go beyond traditional evaluation metrics.

General data protection frameworks such as the EU General Data Protection Regulation (GDPR) [13] and related ethical guidelines provide only high-level principles and are not specifically tailored to the workflows of serious game validation. This creates challenges for researchers in operationalizing compliance requirements during experimental design. Although GDPR aims to strengthen data protection practices, studies show that its practical impact on serious

games research remains limited, with only modest changes in how privacy measures are implemented and reported [20]. Furthermore, research in Learning Analytics demonstrates that even pseudonymized gameplay logs may be vulnerable to re-identification through behavioral pattern analysis and sequence linkage [24].

To support compliance, various tools and frameworks have been developed for data controllers and researchers. These range from general GDPR self-assessment checklists that evaluate organizational readiness for compliance [1], [8], [10], to more specialized software solutions for privacy assessment and security analysis [15], [25], [26]. However, most of these tools remain generic and are not designed to address the specific requirements and complexities of serious game validation workflows. To address this gap, this paper proposes a decision-support framework for compliance-aware serious game validation. The framework allows researchers to structure validation experiments into modular components, specify data processing activities at each stage, and automatically generate GDPR-aligned compliance checklists based on the experimental design. This approach aims to support researchers in integrating privacy and compliance considerations into experimental planning while reducing the complexity of serious game validation processes.

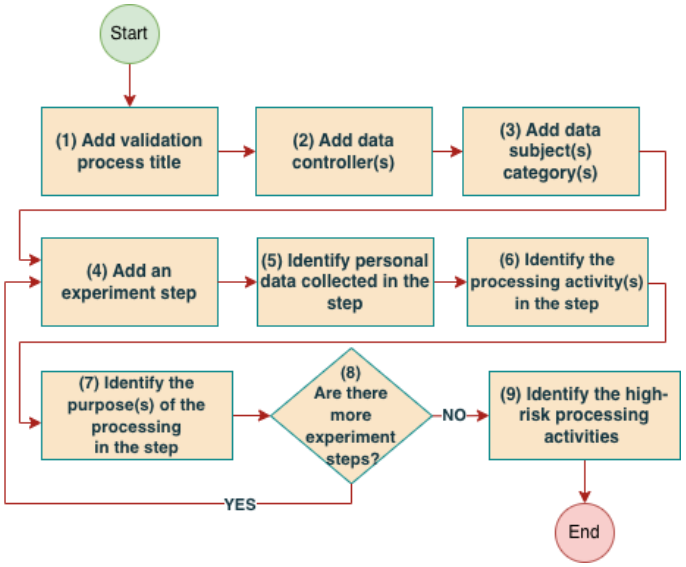


Fig. 1. Flowchart illustrating the process through which researchers answer framework questions to describe personal data processing activities for each step in their experimental design, including data subjects, categories of collected personal data, types and purposes of processing, and to identify potentially high-risk processing activities requiring further GDPR compliance assessment.

## II. Proposed Framework

The proposed framework consists of three main components: (1) structured validation questions, (2) decision logics, and (3) compliance output in the form of obligations and checklist items. The framework operates by guiding researchers through a set of structured questions related to the serious game validation process. Through these questions, researchers specify the characteristics of their validation study. Based on the provided answers, the decision logic maps the validation scenario to relevant obligations. Finally, the framework generates compliance-oriented outputs in the form of recommendations, safeguards, and obligations tailored to the specific serious game validation scenario.

The framework is grounded in three complementary sources: the EU General Data Protection Regulation (GDPR), the UK Information Commissioner's Office (ICO) Game Design Specification, developed with support from *Fundamentally Games* [17], and the Article 29 Working Party (WP29) Data Protection Impact Assessment (DPIA) guideline [4], as endorsed by the European Data Protection Board (EDPB). These sources were selected to integrate legal obligations, domain-specific recommendations, and risk-based privacy considerations relevant to serious game validation.

### A. Structured Questions

**Description of the Validation Scenario and RoPA Construction:** Researchers first describe the characteristics of their validation procedure by following the steps illustrated in Figure 1. At each step, they answer a set of questions, either by selecting from predefined options or by providing their own specific responses.

As illustrated in Figure 1, researchers need to identify: (1) title, (2) data controller(s), and (3) data subject(s) of the validation system. A data controller is the person, organization, or entity that determines why and how personal data is processed. A data subject is any living individual whose personal data is collected, held, or processed within the serious game validation system. The predefined values for data subjects are derived from the Data Privacy Vocabulary (DPV) taxonomy [23], which provides an ontology of terms for characterising different aspects of data processing operations. Researchers can select from options such as *Adults*, *Children*, *Students*, *Employees*, *Job applicants*, and *Vulnerable individuals*.

In Step 4, the researcher defines the first activity in the experimental design, such as a pre- or post-test, interview, gameplay session, or another validation activity. For each activity, Steps 5–7 identify three key characteristics: the collected data, the processing activities, and their purposes. The collected data (Step 5) refers to any information gathered from different sources for the purpose of validating the serious game, including data obtained from data subjects or external sources. Based on the GDPR (Articles 4 and 9 and Recital 30) and the ISO/IEC 29100 privacy framework [18], the options in this section are structured into five categories: *direct identifiers* (such as full name, national ID, and email address); *digital and technical identifiers* (such as IP address, unique device identifiers, and cookies); *demographic and background data* (such as age, gender, and educational level); *performance and behavioural data* (such as pre- and post-test results, in-game telemetry data, open-ended survey responses, and interview transcripts); and *sensitive and biometric data* (such as

physiological signals, media recordings, and special categories of data including but not limited to health status, disability information, and ethnic origin).

The processing activities within each experimental activity (Step 6) are predefined using the DPV taxonomy, which defines a structured list of possible processing operations. DPV includes high-level processing types such as *storing*, *obtaining*, *using*, and *disclosing data*, as well as more fine-grained activities such as *analysing*, *profiling*, and *tracking*, which are particularly relevant in the context of SG validation.

Researchers must also specify the intended purposes of these processing activities (Step 7). For predefined processing purposes in SG validation, we derived a set of data processing objectives from the literature, drawing on [22] and [2], including: *learning and performance assessment*, *behavioural and cognitive analysis*, *system and impact evaluation*, *game design improvement*, and *game adaptation and personalisation*.

In Step 8, the framework verifies whether another experimental activity exists. If the answer is "yes," steps 4 to 8 are repeated. If the answer is "no," the researcher proceeds to the next step. Together, these steps support researchers in maintaining a Record of Processing Activities (RoPA), as required by Article 30 of the GDPR, which mandates documentation of data processing operations and related compliance measures. Some baseline data controller obligations are also identified earlier here based on the specified characteristics of the validation activities.

**Identification of High-Risk Processing Activities (WP29 Criteria):** A key aspect of the GDPR is its risk-based approach to personal data processing, requiring data controllers to assess whether processing activities are likely to pose high risks to individuals' rights and, where necessary, to apply mitigation measures through a Data Protection Impact Assessment (DPIA). To support this, Step 9 of the framework evaluates risk-related characteristics of the validation system that may not be captured in earlier steps, including large-scale profiling, automated decision-making, and data linkage. This enables a broader assessment beyond a simple inventory of processed data by considering contextual risk factors.

We incorporate DPIA-related questions derived from relevant GDPR provisions and WP29 guidelines. The WP29 identifies nine criteria indicating high-risk processing, which are operationalised in the framework as context-specific binary (yes/no) questions tailored to serious game validation. These criteria, along with example questions adapted to the SG validation context are presented in Table I.

### *B. Decision Logic*

The framework adopts a two-layer rule-based decision-making approach in which user responses are mapped to predefined GDPR obligations. The first layer focuses on the general characteristics of the validation system, capturing baseline information about data subjects, data controllers, and data processing activities. Even when all DPIA-related questions are answered negatively, the framework still generates baseline GDPR compliance recommendations, ensuring that compliance coverage is maintained independently of the risk level.

The second layer refines this analysis by assessing risk-related characteristics. Affirmative responses to each question listed in Table I trigger specific rules that activate corresponding GDPR obligations. These rules are available in the online tool[1]. Positive responses also increase the likelihood that the processing activity may be considered high risk, thereby indicating the potential need to conduct a DPIA.

For example, a medical serious game for early dementia assessment collects eye-movement patterns, pupil dilation, and facial responses to evaluate cognitive and neurological performance. Since these biometric and physiological data may reveal health information, they fall under special category data defined in Article 9 GDPR. This triggers obligations for sensitive data processing, including obtaining a valid legal basis such as consent, applying enhanced safeguards such as encryption and access control, ensuring greater transparency, and conducting a DPIA.

TABLE I
THE NINE HIGH-RISK PROCESSING CRITERIA DEFINED IN THE WP29 DPIA GUIDELINE AND EXAMPLES OF SG VALIDATION-RELATED QUESTIONS INCORPORATED INTO THE FRAMEWORK.

| Number | WP29 criteria for risky operations | Example questions within SG validation context |
|---|---|---|
| 1 | Data concerning vulnerable data subjects | Is there a potential power imbalance between researcher/game controller and participants in SG validation? |
| 2 | Sensitive or special categories of personal data | Does the processing activity in this validation step involve any special categories of personal data under GDPR Article 9 (e.g., health-related indicators, biometric signals such as eye-tracking or facial expression data)? |
| 3 | Significant impact on individuals | Does the processing affect individuals' legal rights such as access to services or educational assessment? |
| 4 | Large-scale data processing | Is the number of participants involved in the validation considered high? |
| 5 | Innovative technology | Does the validation use AR/VR, eye-tracking, facial expression tracking, or AI-based analytics? |
| 6 | Automated decision making | Are learning outcomes automatically evaluated for classification or progression decisions? |
| 7 | Systematic monitoring | Is participant behaviour continuously tracked during gameplay sessions? |
| 8 | Evaluation or scoring | Is scoring or profiling performed based on in-game behaviour or user data? |
| 9 | Data set combination | Are multiple datasets combined beyond participants' expectations? |

### C. Compliance Output

The framework generates a customized compliance output, which is a list of necessary action points, by mapping specific obligations to each of the researcher's answers.

The GDPR serves as the primary legal foundation of the framework by defining the core responsibilities of data controllers. We extracted these responsibilities in 8 categories: *Data Subjects Rights, Lawfulness and Fairness, Transparency and Communication, Governance and Accountability, Third-Party and Processing Control, Security and Incident Management, International Data Transfers, and DPIA*. For each category, the necessary action points are extracted from the GDPR itself, WP29, and other relevant resources such as [10] and [16]. Furthermore, to contextualise these obligations within digital games and interactive environments, the framework incorporates recommendations from the ICO-Fundamentally Games Specification. This document provides practical privacy and data protection considerations specifically related to game design, children's data, and player protection mechanisms. These recommendations were used to translate generic GDPR principles into serious-game-specific validation concerns. Table II presents examples of GDPR data controller's responsibilities alongside corresponding considerations derived by ICO-Fundamentally Games Specification. WP29-derived questions, GDPR controller responsibilities, and rule-based obligations triggered by WP29 criteria are available online[1]

TABLE II
EXAMPLES OF GDPR DATA CONTROLLER OBLIGATIONS AND ASSOCIATED ACTION POINTS, WITH CORRESPONDING CONSIDERATIONS FROM THE ICO-FUNDAMENTALLY GAMES SPECIFICATION.

| **GDPR obligation** | **GDPR action point** | **ICO-Fundamentally Games Specification** |
|---|---|---|
| Transparency and Communication | Provide clear, accessible information to data subjects regarding data processing activities. | In case the data subject is a child, ensure privacy information is concise, prominent and written in clear language that a child could understand. |
| Fairness | Ensure that personal data is processed fairly and that the processing does not have unjustified or harmful effects on data subjects. | In case the data subject is a child, design and develop your online service with the best interests of the child in mind, considering age, safety, and wellbeing. |
| Data Protection by Design and by Default | Apply data protection by design and by default in all processing activities. | If applicable, switch geolocation settings to 'off' by default unless necessary, and make location tracking visible. |
| Data Subjects Rights' | Ensure mechanisms are in place to facilitate exercising data subjects' rights. | Provide accessible tools for children to exercise rights and report concerns. |

[1]https://e-ucm.github.io/legalComplianceTool/

## III. EXAMPLE APPLICATION

To illustrate the applicability of the proposed framework, we conceptually applied it to Conectado [7], a serious game developed to raise awareness about bullying and cyberbullying among students between 12 and 17 years old. The player takes the role of a new student who becomes the victim of cyberbullying and bullying at school, with the goal of fostering empathy towards victims. Its story unfolds over five in-game days, during which players interact with classmates and experience emotional challenges that simulate the victim's feelings. We consider the validation scenario described in [3] for Conectado. It includes a pre- and post-test designed to measure the impact of the game.

In the scenario, the age and gender of the students were collected, without processing any directly identifying personal data. However, to ensure the applicability of the use case, we assume that email addresses–considered personal data that can directly identify individuals–are also collected. During the gameplay session, game telemetry data, such as clicks, selected options, and interactions with other characters, are collected and stored. Data were collected to evaluate the game's effectiveness in increasing cyberbullying awareness, assess player experience and engagement, analyse behavioural patterns through gameplay analytics, and support real-time monitoring and design refinement of the game intervention.

To analyse this serious game validation using the proposed framework, the title (validation process for Conectado SG; Figure 1, Step 1), data controller (e-ucm research group; Figure 1, Step 2), and data subjects (children and students; Figure 1, Step 3) are first specified. Subsequently each experimental activity is entered as an input into the framework, followed by the associated collected data, the corresponding processing activities, and their intended purposes (Figure 1, Steps 4 to 8). Figure 2 illustrates this information for the Conectado validation scenario.

Subsequently, the researcher responds to a set of DPIA-related questions (Figure 1, Step 9) to further characterise the validation system, enabling the framework to assess whether the processing activities involve a high level of risk. Due to space limitations, it is not feasible to present the complete set of questions in this paper; therefore, we consider only the representative questions listed in Table I. In Conectado, data subjects fall under the categories of "children" and "students"; therefore, the answer to question 1 is "yes". In addition, in-game telemetry data such as clicks, interactions, and decision-making is collected and combined with responses from the pre- and post-tests. This constitutes behavioural monitoring and tracking. Consequently, the answer to question 7 is "yes". The processing does not involve large-scale operations, the handling of sensitive data, or the use of novel or emerging technologies, such as AI-based algorithms. Furthermore, although a dashboard is used to visualise players' progress, the system does not evaluate, score, or predict any characteristics of data subjects.

Specific answers provided when describing the experimental

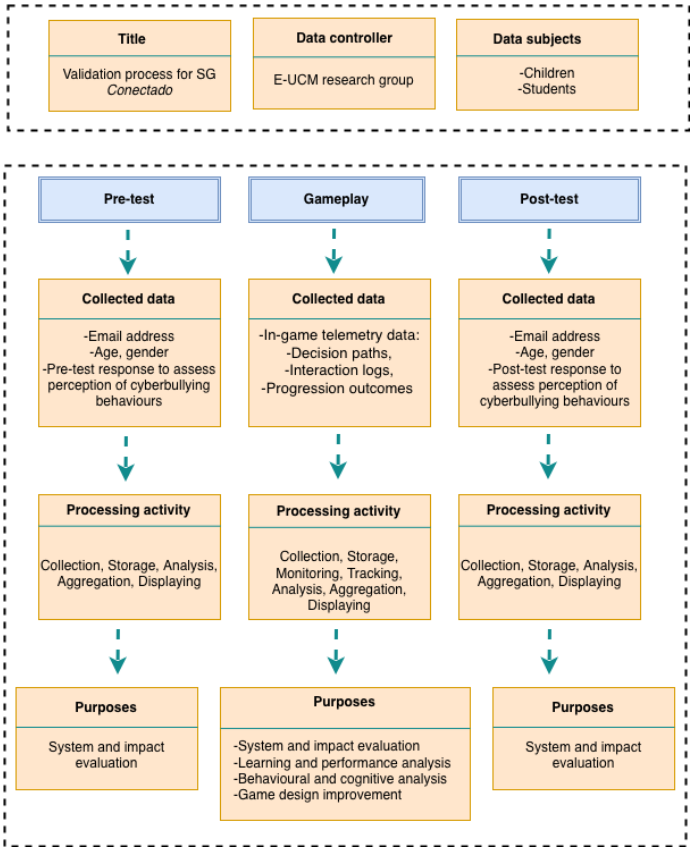


Fig. 2. Example application of the proposed framework to the Conectado serious game validation process, illustrating the experimental design steps, categories of collected personal data, associated processing activities, and the corresponding processing purposes throughout the validation workflow.

activities in the first set of questions (e.g., indicating processing of special categories of data such as health data), as well as positive responses to each of the DPIA-related questions, trigger corresponding categories of obligations under the GDPR. In the example presented above, specifying data subjects as "children" and affirmative answers to questions 1 and 7 activate obligations related to: (i) the processing of children's personal data, and (ii) systematic monitoring and profiling activities. Below, we present an excerpt of the recommendations in the compliance output generated by the framework. Each recommendation is formulated in accessible and concise language, avoiding unnecessary legal terminology, while also specifying the relevant regulatory reference and the triggering condition associated with the obligation.

*Compliance output for "validation process for SG Conectado" by "e-UCM research group"* :

- **Obligations triggered by processing of children's personal data:**
  - Ensure that children under 16 (or lower if a Member State sets) obtain parental consent for online services processing personal data (Art. 8 GDPR).
- **Obligations triggered by systematic monitoring:**
  - Ensure participants are explicitly informed about systematic behavioural monitoring in digital environments, including logging of gameplay actions and interaction traces (Art. 13–14, Recital 75).
- **Obligations triggered by both**:
  - Ensure mechanisms for data subject rights are available, including access, rectification, erasure, restriction, and objection to processing where applicable (Art. 15–21). Provide prominent and accessible tools to help children exercise their data protection rights and report concerns (ICO-Fundamentally Games Specification).
  - Ensure Data Protection by Design and by Default is applied, including privacy-preserving configuration of data collection, storage, and analysis pipelines (Art. 25). Set all privacy settings to 'high' by default, unless you can demonstrate a reason not to, and avoid nudge techniques that encourage unnecessary data disclosure or weakening of privacy protections (ICO-Fundamentally Games Specification).
  - Conduct a Data Protection Impact Assessment (DPIA) where processing is likely to result in high risk, especially when involving children or systematic monitoring (Art. 35, Recital 75, WP29 DPIA Guidelines).

## IV. Discussion and Future Work

In this paper, we proposed a framework to help serious game developers and researchers understand potential data protection obligations in relation to their serious game validation processes. The framework translates abstract GDPR concepts into operational, context-specific questions. It is designed for early-stage experimental design, prior to implementing technical and organisational measures such as pseudonymisation or consent management. At this stage, it enables the identification of privacy risks and DPIA-relevant scenarios before data collection takes place. By offering structured guidance, the framework reduces dependence on specialised legal expertise and supports privacy-by-design principles in accordance with Article 25 GDPR. Comprehensive empirical validation is left for future work. Nevertheless, the example application demonstrates the framework's applicability in real-world validation scenarios and its potential to support early-stage serious game study design.

The framework is grounded in the GDPR and relevant WP29 guidance, but it does not provide interpretations beyond those set out in these sources, nor does it constitute an authoritative legal assessment. Where the GDPR leaves room for interpretation, the framework relies on WP29 guidance to operationalise key concepts. For instance, while the GDPR specifies that parental consent is required for children under the age of 16 in relation to online services (with Member States allowed to lower this threshold to 13), it does not provide a precise legal definition of "children" beyond this operational boundary. Consequently, some assessments may still involve

a degree of contextual interpretation by the researcher. Moreover, the framework does not incorporate an explicit risk-scoring mechanism. In practice, different processing activities may entail varying levels of risk to individuals and their personal data. For example, monitoring the online behaviour of millions of players during gameplay and collecting gameplay data from a small group of 14 students in a local school may both be considered processing activities involving some level of risk; however, the former typically involves a substantially higher risk due to its large scale and the potentially greater impact in the event of a security incident. The current version of the framework does not differentiate between such variations in risk magnitude. Instead, it adopts a deliberately conservative design approach, whereby it may indicate the need for a DPIA even in relatively low-risk educational serious game scenarios.

Future work will extend the proposed framework in several directions. First, it could be implemented as a software tool that enables researchers to input system characteristics and obtain automated, structured compliance outputs based on the decision logic. Second, the framework could be enhanced with a risk-weighting mechanism that accounts for the scale, sensitivity, and impact of data processing activities, addressing its current conservative design. Finally, future extensions may incorporate AI-related ethical considerations in serious games, extending compliance beyond GDPR to include AI ethics and human-centred design perspectives informed by frameworks such as the Artificial Intelligence Act [14] and the Assessment List for Trustworthy Artificial Intelligence (ALTAI) [12].

## Acknowledgment

This work was partially funded by the Ministry of Education (PID2023-149341OB-I00), and by the Telefonica-Complutense Honorary Chair on Digital Education and Serious Games.

## References

[1] Agencia Española de Protección de Datos (AEPD): Listado de cumplimiento del rgpd (2018), https://www.aepd.es/guias/guia-listado-de-cumplimiento-del-rgpd.pdf, gDPR compliance checklist and self-assessment guide, accessed 2026-05-19

[2] Alonso-Fernández, C., Calvo-Morata, A., Freire, M., Martínez-Ortiz, I., Fernández-Manjón, B.: Applications of data science to game learning analytics data: A systematic literature review. Computers & Education **141**, 103612 (2019)

[3] Alonso-Fernández, C., Cano, A.R., Calvo-Morata, A., Freire, M., Martínez-Ortiz, I., Fernández-Manjón, B.: Lessons learned applying learning analytics to assess serious games. Computers in Human Behavior **99**, 301–309 (2019)

[4] Article 29 Working Party: Guidelines on data protection impact assessment (dpia) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679 (2017), https://ec.europa.eu/newsroom/article29/items/611236, adopted on 4 April 2017, last revised and adopted on 4 October 2017. Accessed: 2026-05-17

[5] Bellotti, F., Kapralos, B., Lee, K., Moreno-Ger, P., Berta, R.: Assessment in and of serious games: An overview. Advances in Human-Computer Interaction **2013**(1), 136864 (2013)

[6] Calderón, A., Ruiz, M.: A systematic literature review on serious games evaluation: An application to software project management. Computers & Education **87**, 396–422 (2015)

[7] Calvo-Morata, A., Alonso-Fernández, C., Freire, M., Martínez-Ortiz, I., Fernández-Manjón, B.: Creating awareness on bullying and cyberbullying among young people: Validating the effectiveness and design of the serious game conectado. Telematics and Informatics **60**, 101568 (2021)

[8] Commission Nationale de l'Informatique et des Libertés (CNIL): Gdpr toolkit (2026), https://www.cnil.fr/en/my-compliance-tools/gdpr-toolkit, gDPR compliance tools and guidance (accessed 2026-05-19)

[9] Connolly, T.M., Boyle, E.A., MacArthur, E., Hainey, T., Boyle, J.M.: A systematic literature review of empirical evidence on computer games and serious games. Computers & education **59**(2), 661–686 (2012)

[10] Data Protection Commission Ireland: Self-assessment checklist for organisations (nd), https://www.dataprotection.ie/en/organisations/resources-organisations/self-assessment-checklist, accessed: 2026-05-19

[11] Drachen, A., Thurau, C., Togelius, J., Yannakakis, G.N., Bauckhage, C.: Game data mining. In: Game analytics: Maximizing the value of player data, pp. 205–253. Springer (2013)

[12] European Commission High-Level Expert Group on Artificial Intelligence: Assessment list for trustworthy artificial intelligence (altai) for self-assessment. Tech. rep., European Commission (2020), https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

[13] European Parliament, Council of the European Union: 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) (2016), http://data.europa.eu/eli/reg/2016/679/oj

[14] European Parliament and Council of the European Union: Artificial intelligence act. Regulation of the European Union (2024), https://eur-lex.europa.eu/eli/reg/2024/1689/oj, regulation (EU) 2024/1689

[15] Fan, M., Yu, L., Chen, S., Zhou, H., Luo, X., Li, S., Liu, Y., Liu, J., Liu, T.: An empirical evaluation of gdpr compliance violations in android mhealth apps. In: 2020 IEEE 31st international symposium on software reliability engineering (ISSRE). pp. 253–264. IEEE (2020)

[16] GDPR.eu: Gdpr compliance checklist (nd), https://gdpr.eu/checklist/, accessed: 2026-05-19

[17] Information Commissioner's Office: Fundamentally games: Data protection and video games guidance. https://ico.org.uk/media2/migrated/4018787/ico-game-design-spec.pdf (2026), accessed: 2026-05-17

[18] International Organization for Standardization, International Electrotechnical Commission: ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework (2011), international Standard

[19] Jost, P., Divitini, M.: Designing analytic serious games: an expert affordance view on privacy decision-making. In: Joint International Conference on Serious Games. pp. 3–19. Springer (2021)

[20] Jost, P., Lampert, M.: Two years after: A scoping review of gdpr effects on serious games research ethics reporting. In: International Conference on Games and Learning Alliance. pp. 372–385. Springer (2020)

[21] Khosravi, H., Viberg, O., Kovanovic, V., Ferguson, R.: Generative ai and learning analytics. Journal of Learning Analytics **10**(3), 1–6 (2023)

[22] Loh, C.S., Sheng, Y., Ifenthaler, D.: Serious games analytics: Methodologies for performance measurement, assessment, and improvement, vol. 264. Springer (2015)

[23] Pandit, H.J., Esteves, B., Krog, G.P., Ryan, P., Golpayegani, D., Flake, J.: Data privacy vocabulary (dpv)–version 2. arXiv preprint arXiv:2404.13426 (2024)

[24] Pardo, A., Siemens, G.: Ethical and privacy principles for learning analytics. British journal of educational technology **45**(3), 438–450 (2014)

[25] Pereira, F., Crocker, P., Leithardt, V.R.: Padres: tool for privacy, data regulation and security. SoftwareX **17**, 100895 (2022)

[26] Piras, L., Al-Obeidallah, M.G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., Bernard, J.B., Fiorani, M., Magkos, E., Sanz, A.C., et al.: Defend architecture: a privacy by design platform for gdpr compliance. In: International conference on trust and privacy in digital business. pp. 78–93. Springer (2019)