Principles on Children & Online Gaming

June 2024

Foreword

On 13–14 October 2022, a Nordic Data Protection Meeting was held in Helsinki to discuss current issues in the field of data protection and to share experiences. The Nordic Data Protection Authorities (DPAs) adopted the “Helsinki Declaration”, in which it was agreed that the protection of children’s data was a priority for the Nordic DPAs.

The Danish DPA drew attention to the findings of a think-tank report by the Danish Society Engineers and DataEthics.eu on Game-Tech, Data and Children that shed light on the need for better protection of the rights of children playing digital games.

In light of the growing digital gaming industry, including in the Nordic countries, the Nordic DPAs decided to form an informal working group related to children and online gaming. The group was, first of all, to consider joint awareness-raising and guidance activities to promote children’s data protection rights.

The working group has particularly focused on the need to provide basic guidance to data controllers who must ensure that children are provided the protection that they are entitled to when designing and developing digital games. The principles below are the result of the Nordic cooperation, as decided in Helsinki in October 2022.

Introduction

As online gaming becomes increasingly accessible, so does its ability to open up positive experiences for all kinds of players. However, online gaming also opens up important questions about privacy and the protection of personal data, particularly when they are being played by children.

It is therefore vital that controllers—the ones who determines the "how and the why" of the data processing—embrace their responsibilities under the General Data Protection Regulation (the GDPR) to protect the personal data of their players, and to take special consideration when processing personal data that relates to children. This applies whether or not the controller intends that children can access their game and the GDPR does not distinguish between the deliberate or the accidental processing of personal data relating to a child. As stated in Recital 38 GDPR, "children merit specific protection with regard to their personal data"; this is not just something that controllers should do, it is something that they must do.

This document will provide some starting guidance for the GDPR-compliant processing of personal data in the context of children and online gaming. In it, we will explore four of the data processing principles set out under the GDPR—**fairness, transparency, data minimisation and accountability**—and will set out a number of important questions and considerations for controllers. We do not here intend to be exhaustive; not only do other data processing principles exist, the principles are all deliberately general in nature and will require different implementations in different circumstances. Equally, while the four principles discussed here are important, they complement, rather than replace, the other provisions in the GDPR. It is therefore up to controllers to thoroughly examine their processing activities and determine what they must do to be compliant with the law and with rights of their players.

Each section will review the principle in question, consider why it is important, and then explore how that principle relates to the GDPR. It will then offer a number of questions, points or considerations that can help controllers to promote that principle in their processing activities. By engaging with these prompts in a full and meaningful way, controllers can develop their processing activities in a way that helps to protect their players' personal data.

Article 5 Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, **fairness** and **transparency**');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**').

Definition of key terms

- **'(Data) Controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing is determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- **'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;

- **'(Data) 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;

- **'Data protection by design'** means implementing appropriate technical and organisational measures such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

- **'Data protection by default'** means implementing appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

- **'Child'** means every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier.

- **'Online gaming'** should be understood broadly. This could include, among other things, both multiplayer and singleplayer online games; games which run on general-purpose devices (such as phones, tablets, PCs or consoles) and games which run on single- or specific-purpose devices or hardware; and games which are themselves presented as the end-product and games which are themselves integrated into another product or service

Fairness

1. What is the principle of fairness?

The principle of fairness is one of three elements contained in Article 5(1)(a) GDPR and must be applied to all processing activities. Fairness under the GDPR is specific to the processing of personal data and therefore does not, for example, mean that everything in the entire consumer relationship must be fair per se. Equally, whether something is fair remains a legal question and should not be taken as unbridled discretion to arbitrarily declare something as unlawful. Nevertheless, what is considered "fair" depends on a case-by-case analysis and controllers must think about the specific circumstances surrounding their processing activities and the children involved. Fairness is particularly important when it comes to children and other potentially vulnerable people; in some circumstances, you must be extra careful about the way that you use personal data, and fairness is one way to gauge how those extra protections should be applied. Fairness is important because it can act as a lens on the situation, ensuring that the protection of personal data is appropriate to the specific circumstances at hand.

2. How does fairness relate to the GDPR?

Under Article 5(1)(a) GDPR, all processing of personal data must be done fairly. As with the other principles set out under Article 5, this can impose an absolute requirement of fairness ("Your processing must be fair, no matter what") and act as a lens for interpreting other provisions in the GDPR ("My implementation of this right must be done in a way that is fair").

When there may be a conflict between different rights or interests, the GDPR requires you to resolve that conflict in a way that is fair for children. This could, for example, include a conflict between a game developer's interest in learning about their players and a child's interest in protecting their personal data; the question is not "which side wins?" but "how do we fairly resolve this conflict?". Sometimes fairness will require a compromise, imposing modifications, restrictions or safeguards on the processing activity so that it achieves a broadly-similar purpose but does so in a more privacy-friendly way. Sometimes, however, fairness will require a stricter approach and may prevent the processing activity altogether. When making this evaluation, it is very important that you consider the players' reasonable expectations, as it is unlikely that something will be considered fair if the player could not have reasonably expected it to happen.

Some helpful questions to ask when thinking about fair processing:

- What does my processing activity involve?
- Have I identified the children (or groups of children) who might be affected by my processing activity? If appropriate, have I consulted those children, or those who might be able to speak on their behalf?
- How does my processing activity affect those children? What are the positives and negatives and how might different children be affected?
- Are the benefits of my processing activities fair in light of the potential impacts? Would the affected children agree with my analysis? Would I be happy with the processing activity if I were in those children's position?

These are not the only things to consider. Make sure you look at the specifics of your own processing activities and consider what may or may not make the processing unfair!

3. How can you promote fairness in your processing activities?

Evaluating fairness will, inevitably, require a comprehensive look at the processing activity and all of the circumstances surrounding that activity. It is impossible to create a comprehensive list of things to consider as each case of fairness must be evaluated on the specific facts themselves. When it comes to children and online gaming, the following starting points may be helpful:

- Think carefully about what you want to do in your game. Not everything needs to benefit everyone equally, but in order for processing to be fair to everyone, you should ensure that the processing is not unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the child, or in a way that uses personal data to manipulate children to act against their interests (e.g. by nudging them towards purchase decisions or by encouraging addictive behaviour).

- Think carefully about the places where fairness might require you to take extra steps to protect your players' data. It's possible that something about your game is particularly risky or impactful for certain vulnerable groups, including children. You will need to find a way to control for those factors to keep your processing of personal data fair for everyone.

- Think carefully about your specific audience. Children are not a homogenous group, and different factors like age, upbringing and personal circumstances can have a large effect on what is or is not fair. It may be that your audience is made up of several different groups of children so that something which is fair for some of the players would be unfair for others. For example, children in different age or development ranges who play the same game will require different age- or development-appropriate measures. Make sure to think about your own blind spots and find a way to control for them (e.g. by consulting people who might have a different perspective to your own).

- Think carefully about the way that you design your interfaces and player experience. Children can be particularly vulnerable to deceptive or manipulative design patterns and language, and should not be nudged towards options which (either directly or indirectly) involve extra or increased processing of personal data. This may, for example, mean that you should avoid features or design choices that nudge children to maximise their engagement with the game, by use of their personal data.

- Think carefully about the unintended or indirect consequences of your game. The processing of personal data can have wide or unexpected consequences for data subjects and these may affect your various obligations under the GDPR. You will need to think about your processing activities within this wider context to make sure that your processing is fair and that you are properly respecting children's data protection rights.

- Think carefully about both the substantive and the procedural aspects. For example, when asking children if they want their profile to be public or private, you need to make sure that both the way that you ask and the consequences of that choice are fair.

Transparency

1. What is the principle of transparency?

Transparency is an overarching principle and a key obligation under the GDPR. In short, you have a duty to demonstrate that personal data is processed in an open and honest manner. This entails that you must provide concise and comprehensible information about the data processing at all stages of the data processing cycle.

The information given to the child must be easily accessible and easy to understand. The language used must be clear and plain. The duty to provide information applies regardless of the child's age and development; the main goal is that the child is able to understand how their personal data is being used.

Transparency is also closely linked to the principle of fairness. If you are not clear and transparent about how you process children's data, it is unlikely that your processing will be considered fair.

2. When should we give the information/at what stage?

When the personal data is collected directly from the child, information about the processing must be given at the time when the personal data is obtained. In practice, many games collect personal data both when creating an account and every time the user engages with the game/platform. This means that information should be available and/or provided at all of these stages.

If you collect personal data about the child from other sources than the child themself, the information must be provided within a reasonable period after obtaining the personal data, but at the latest within one month.

Amongst other things, you need to provide the following information about the processing:

- where the data is collected from - the child or other sources,
- why data is collected, e.g., for what purposes,
- the legal basis that allows you to process the data,
- who will receive the data,
- the most important consequences of the processing and how it will affect the child's experience when using the service,
- the retention period, and
- how the child can exercise their data protection rights.

A more comprehensive list of the requirements can be found in Article 13 and 14 GDPR, depending on where the data is from.

3. How can you promote transparency?

Promoting transparency is an ongoing task, and you should regularly review if the information you provide is updated and adequate. When it comes to children and online gaming, the following starting points may be helpful:

- Think carefully about how you can promote transparency and children's need for specific protection all stages of the design cycle to ensure that your service meets the requirements in the GDPR. For example, you can:
  - make privacy information a part of the design of the service, so that it does not feel separate to the design of the service or take the children away from their core activity,
  - provide privacy information in bite-sized portions at relevant points of the user journey, and
  - ensure child participation at different age levels when designing your service to get their feedback on which measures to implement.

- Think carefully about how you present the information. One way to promote transparency is to have a separate privacy notice for children, where the language and form are adapted to children's level of understanding, in addition to one at the level for parents and legal guardians. It may be useful to or required to consider the following to make the information easier for the child to understand:
  - Display transparency information based on ability rather than age. For example, transparency information at beginner, intermediate, and expert levels. It is also possible to include a "I don't understand"-button, opening a pathway for children to request more or less complex information,
  - Use illustrations, videos and/or examples to make it easier for the child to understand and to attract their interest,
  - Avoid information overload by providing layered information where it is relevant and needed,
  - Provide clear explanations of user control choices and default settings (data protection by default),
  - Inform the children whom to ask if they have questions, and
  - Include a short quiz or other measures to ensure the child has understood the information provided.

- Think carefully about giving information about what information you process and how decisions regarding age verification are made, if you process data for age verification purposes.

- If parental controls are in place, information about this should be given to the child so the child knows what the parents may see or have access to.

- Think carefully about giving information about processing of children's data for decision-making purposes, in particular about what information you process, how decisions are made and how the individuals can review the data and edit it if needed. In this context, it is also important to remember that children should never be subject to a decision which is based solely on automated processing and which produces legal effects concerning them or similarly significantly affects them. For example, the situation when a child gets banned from an online game due to an automated decision making and it hasn't been reviewed by a human and the child loses access to the product.

Data minimisation

1. What is the principle of data minimisation?

In practical terms, the principle of data minimisation requires that you limit the volume of personal data, as well as the types, categories and level of detail of personal data, to that necessary for the processing purpose(s).

This means that you must only process the minimum amount of personal data to provide the elements of the game for the purposes of playing the specific game for example to avoid harassment within the game. It also means minimising the subsequent processing of data – especially in regard to subsequent sharing of personal data with third parties, such as external support teams.

2. How can you promote data minimisation when developing the game?

Already when developing and designing the game, you need to take the necessary steps to ensure that the processing of children's data is carried out only for what is essential for the functions of the services.

This means that you should ensure that in-game settings interfering with the child's privacy and data protection rights are turned off by default. In the context of gaming this includes avoiding tracking of geographic location, access to contacts, voice recording, synchronization with social media, etc. as standard settings unless fundamentally necessary for the purpose(s) of playing that specific game.

The nature of games generally entails that the more time and attention the child uses on each game, the more personal data about the child it will generate. Online games can collect a wide range of personal data concerning the child through its actions within the game, including embedded software codes from third parties.

Instead of automatically collecting and analyzing this data, for example, with a view of predicting "types of players", deriving data on the child's personality, cognitive abilities, etc. you should consider ways to achieve the purpose by processing less personal data, e.g. giving the child a choice as to what genres of games they are interested in, what difficulty level they want to play etc.

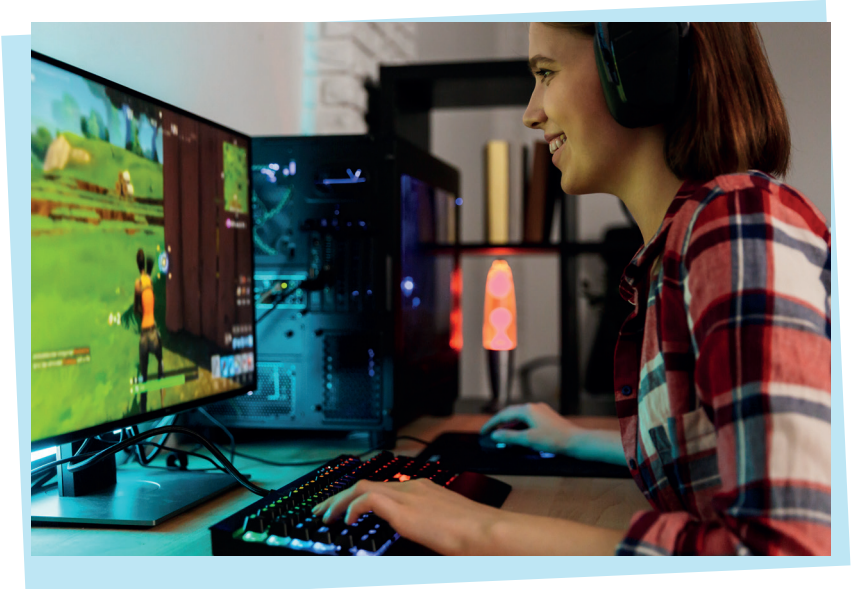
3. How can you promote data minimisation within the game?

- Always think of less extensive and less intrusive ways to achieve your purposes. You should not process children's data if it is not necessary for the purpose(s) you pursue. In many cases, it may be possible to avoid processing the child's personal data altogether or to use a more data protection friendly approach. For example, if you are processing personal data to protect account security, make sure to consider whether you actually need every piece of data processed. For example, you should ask whether it is necessary, in your specific circumstances, to gather information about the specific device which is being used to connect to the game, or whether some kind of password and/or 2FA would be sufficient.

- Apart from the collection of personal data for the core of the game, you should give the child as much control as possible in terms of which additional features or enhancements of your game they wish to use and, as a result, the amount of data the child has to provide. Even where the child is given these choices, it is important to remember that the high-privacy options should be used as the default settings.

- Think carefully about demonstrating that you have collected only the personal data relevant and limited to what is necessary for your specified purposes and how the rights and interests of child users have guided the design and development of the game. Your documentation must reflect the considerations and choices that you have made in the context of data protection as explained in the section on accountability.

- Think carefully about processing personal data for age verification purposes. If you need to process data for establishing the player's age, the processing must be limited to the minimum amount of personal data necessary for that particular purpose. Specifically, you must not use age verification as cover for aggressive data collection practices or as an excuse to avoid implementing children's entitlements.



Accountability

1. What is the principle of accountability?

The accountability principle aims to guarantee compliance with the GDPR. It requires you, as the data controller, to take responsibility for your processing operations and you must be able to demonstrate your compliance. More specifically you need to be able to demonstrate compliance with the GDPR, including the principles relating to processing of personal data, set out in Article 5(1) GDPR. The principle of accountability is also enshrined in Article 24 GDPR.

In practice, the accountability principle requires you to assess and implement appropriate and effective technical and organisational measures to ensure compliance with the principles and obligations set out in the GDPR. As emphasised in the preamble of the GDPR, children merit specific protection in relation to their personal data. This higher standard of protection derives in part from Article 24, which requires that you take into account the risk of varying likelihood and severity for the rights and freedoms of individuals when assessing and implementing appropriate measures. When you process children's personal data, you should identify the risks specific to children and implement effective measures to safeguard against those risks. These measures should be risk-based, proportionate and they must be reviewed and updated where necessary.

2. How to promote accountability in your processing activities?

You must be ready to demonstrate that you are compliant with the GDPR. Namely, you should be able to, at any time, provide documentation regarding specific measures you have taken to guarantee compliance with the principles of GDPR. Below you can find a description of some key requirements and a list with examples of measures to consider. Any such measures must be recorded and documented. When it comes to children and online gaming the following starting points may be helpful:

- Think carefully about the need to carry out a data protection impact assessment (DPIA) to systematically identify, assess and mitigate risks to the rights and freedoms of children, that arise from your data processing. In many cases it may be mandatory for you to carry out such an assessment.
  - A DPIA should be carried out during the design and development of your game and before you begin any type of processing that is likely to result in a high risk to the rights and freedom of children.
  - A DPIA shall describe the purpose of the online game or feature, how it uses children's personal data, and the risks to children that arise from the data processing.
  - A DPIA can help you implement data protection by design into the processing by identifying risks at an early stage.
  - A DPIA should also consider broader risks to the rights and freedoms of children including the potential for any significant material, physical, psychological or social harm. To assess the level of risks, both the likelihood and the severity of any impact on children must be considered.
  - Keep records of your DPIA. An effective DPIA can demonstrate that you have considered and mitigated the risks arising from your processing operations.

- Think carefully about documenting the details of the design choices and the security measures you have put in place to guarantee compliance with the GDPR and be ready to demonstrate their effectiveness.

- Think carefully about using prominent and age-appropriate tools for children to exercise their data protection rights and report their concern. These tools should be effective as well as easy to find and use, and, where appropriate, include mechanisms to track progress of the request.

- Think carefully about keeping records of internal policies and procedures that demonstrate how your organisation ensures compliance with the GDPR e.g., in relation to the obligation under Article 30(1) to keep records of your processing activities. As well as drafting data protection policies, you should also be able to show that you have implemented and adhered to them.

Annex 1: Further reading

We have collected some sources for further reading, for those of you who are interested in a deep dive into the topics covered in this document.

1 DATA PROTECTION

Christopher Kuner and others, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

Council of Europe, *European Handbook on Data Protection* (2018 edn)

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] OJ L119/1

2 CHILDREN AND THE INTERNET

University of Leiden & Waag organisation, *Code for Children's Rights* (Dutch Ministry of Interior and Kingdom Relations (2021)

Commission Nationale de l'Informatique et des Libertés (CNIL), *Digital rights of children* (9 August 2021)

Swedish Authority for Privacy Protection (IMY), Ombudsman for Children in Sweden and Swedish Media Council, *The rights of children and young people on digital platforms – Stakeholder guide* (2021)

Information Commissioner's Office (ICO), *Age appropriate design: a code of practice for online services* (Version 2.1.36, 17 October 2022)

Information Commissioner's Office (ICO), *Age assurance for the Children's code* (Version 1.0.2, 15 January 2024)

Danish Society of Engineers' Working Group on Ethics and Technology & DataEthics.eu, *Report on GameTech, Online Games Gamble With Children's Data* (2021)

3 DATA MINIMISATION

European Data Protection Board, *Guidelines 4/2019 on Article 25 Data protection by Design and by Default* (Version 2.0, 20 October 2020)

Case C-252/21 *Meta Platforms Inc v Bundeskartellamnt,* ECLI:EU:C:2023:537

4 FAIRNESS

European Data Protection Board, *Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited* (Art. 65 GDPR) (2 August 2023)

European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (Version 2.0, 20 October 2020)

European Data Protection Board, *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them* (Version 2.0, 14 February 2023)

Case C-252/21 *Meta Platforms Inc v Bundeskartellamnt*, ECLI:EU:C:2023:537

5 ACCOUNTABILITY

Data Protection Commission, *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing,* (Data Protection Commission, December 2021)

Article 29 Data Protection 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 WP248 rev.01,* (4 October 2017, endorsed by European Data Protection Board on 25 May 2018)

6 TRANSPARENCY

Article 29 Data Protection Working Party, *Article 29 Working Party – Guidelines on transparency under Regulation 2016/679, WP250 rev.01* (11 April 2018, endorsed by the European Data Protection Board on 25 May 2018)

Information Commissioner's Office (ICO), *Designing data transparency for children, Insights from the Children's Code transparency champions open call* (2021)

Adopted at the Nordic Data Protection Meeting in Oslo

30 May 2024