DATAETHICS

Report on GameTech

ONLINE GAMES GAMBLE WITH CHILDREN'S DATA

Published by
the Danish Society
of Engineers' Working Group
on Ethics and Technology
& DataEthics.eu

Contents

1. Background 4
1.1. Definition of gaming 5
1.2. Children's rights, the GDPR and data ethics 5
1.3. Danish children and gaming 7

2. Digital games and use of data 8
2.1. Microtargeting 8
2.2. Business models 9
2.3. The ecosystem 10
2.3.1. Game development companies 10
2.3.2. The game engine 12
2.3.3. Gaming devices 13
2.3.4. Actors in advertising 14
2.4. Lack of transparency 14

3. Advertising and manipulation 15
3.1. Persuasive game design 15
3.2. Advertising 15

4. Three popular games 18
4.1 Gaming services disclaim responsibility 18
4.2. Fortnite 19
4.3. Subway Surfers 20
4.4. Candy Crush Saga 21

5. Conclusion and recommendations 22
5.1. Conclusion 22
5.1. Recommendations 23
5.2. Particularly for parents 24

Annex 1 25
Questions to the Danish Data Protection Agency 25

Endnotes 28

"The way mobile games collect information about their users, and the details of what type of information they're collecting, remains incredible opaque (...) The fact that it's all so confusing is kind of the point, obviously. As a result, mobile games have escaped the level of scrutiny we've applied to social media companies, despite being – as category – nearly equally popular and far more likely to be used by children".

Kaitlyn Tiffany, journalist covering technology and internet culture for Vox Magazine, May 2019

1. Background

In May 2020, Reuters[1] reported about a booming global digital gaming market. The market is expected to generate USD 159.3 billion in revenue in 2020 and surpass USD 200 billion in 2023. The launch of the next-generation consoles towards the end of 2020 is also a key contributing factor in the overall growth projections, but the biggest growth is in mobile gaming.

Out of estimated 2.7 billion gamers worldwide, 2.6 billion are playing on mobile devices. Apparently, only 38% will pay to play on their mobil devices[2]. Thus other business models come into play when companies are to profit from the many gamers.

This report will take the first steps in investigating these underlying business models with specific focus on data ethics and children. We use the phrase first steps, as it is not within the scope of this report to conduct technical tests in order to document and analyse the transmission of data between children, games, gaming platforms, and the actors – so-called third and fourth parties – that are part of the complex digital gaming ecosystem. However, there is definitely a need for such an analysis.

This report sheds light on a very complex, opaque ecosystem of gametech actors, all of which play a more or less invisible role in the games Danish children spend hours on every day. The games are entertaining and free to use at first. However, they are based on business models that often fail to consider that children have other needs and rights to claim protection of their data than those of adults.

As the report shows, there is a need for much more transparency in the underlying business models based on advertising technology, as well as transparency in

interpretation and enforcement of existing legislation. Equally, there is also a need for much more critical discussion of how we can protect children in the deeply commercial, data-driven and algorithmically curated world of online gaming.

1.1. Definition of gaming

This report is in line with UNICEF's definition[3] of gaming: 'Online gaming' is defined as playing any type of single - or multiplayer commercial digital game via any Internet-connected device, including dedicated consoles, desktop computers, laptops, tablets and mobile phones. The 'online gaming ecosystem' is defined to include watching others play video games via e-sports, streaming or video-sharing platforms, which typically provide options for viewers to comment on or interact with the players and other members of the audience.

As UNICEF writes, children's gaming experience often involves watching others play, for example on YouTube (owned by Google) or Twitch (owned by Amazon). Here, children spend time streaming themselves, watching their friends stream or following their favourite gaming influencer. They can access Twitch via their computer, gaming console (PlayStation, for example) or smartphone[4]. For space reasons, we will not go into further details about streaming, as this can be said to constitute an ecosystem in itself. The overall topic "children and online gaming" also covers several other relevant areas that require more critical attention. We list some of these under recommendations, as they require separate analyses, but we can already mention that this report will not go into topics such as 'gaming vs gambling' and 'addiction or problematic gaming behaviour'.

1.2. Children's rights, the GDPR and data ethics

Children have a right to demand more protection than adults in all aspects of life. Many countries have signed up for this in the United Nations Convention on the Rights of the Child; the most ratified treaty in history. This also has implications for children's use of data-driven technologies.

According to Article 31[5] of the United Nations Convention on the Rights of the Child, children have a right to participate in cultural and creative activities. This could be interpreted as the child's right to use both social media and digital games when they have reached the age of digital consent. However, children also have a right to be protected and free from economic exploitation and other forms of exploitation prejudicial to the child's welfare, see Articles 32 and 36 of the United Nations Convention on the Rights of the Child. The Convention also concerns privacy, see Article 16. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and here abuse of children's personal data may be an example of a breach of the United Nations Convention on the Rights of the Child. According to the Convention, children must also have access to information and be protected from information which might be injurious to their wellbeing, see Article 17. This

may mean that children have a right to be protected and shielded from digital marketing of products and services or commercial content.[6]

Children are simply easier to manipulate than adults (see more in section 3.0), and therefore it is important that actors in the gametech ecosystem understand and assume responsibility for the potential impact of their products and the underlying business methods on children. According to UNICEF, there is no comprehensive global review or mapping of the impacts of online gaming on children's rights.[7]

Children's rights to protection of their personal data are partly covered by the General Data Protection Regulation (GDPR). Anyone who obtains and processes information about children must comply with the requirements in the GDPR for purpose limitation, necessity and proportionality, and they must have a legal basis for processing. The GDPR states that children can give consent to the processing of their personal data in information society services, i.e. digital consent, from the age of 16 years. This rule has been implemented because children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child, explains the Danish Data Protection Agency in a reply to DataEthics.eu (annex 1). However, Member States may set the age of consent to 13 years. This is the case inIn Denmark, where the age of consent has been set to 13 years in the Danish Data Protection Act.

The question is whether companies are trying to circumvent this responsibility by marking their digital products "not suitable for children under 13 years of age" in their conditions of use.

The European Commission writes[8] that *"Companies have to make reasonable efforts, taking into consideration available technology, to check that the consent given is truly in line with the law. This may involve implementing age-verification measures such as asking a question that an average child would not be able to answer or requesting that the minor provides his parents' email to enable written consent"*. In other words, companies have a duty to obtain parental consent or other forms of age verification to ensure that their data collection and processing are lawful. According to the Danish Data Protection Agency, no cases have tested this yet. Currently, a child can therefore only safeguard themselves fully against monitoring, data collection and microtargeted advertising by not downloading apps or not playing the games at all.

In recent years, especially at international level, there has been specific focus on minors' use of social media and the lack of protection for children and their data.

But there has been no similar focus on gaming and data ethics. This may seem something of a paradox, as the same digital advertising-driven business models are in play. Perhaps it seems more obvious that you share data when you share pictures of yourself on social media, while it is not so obvious what companies actually "charge" from users in connection with online games. But data from games can be equally useful. In other words: games financed by advertising "charge" personal data as payment.

Annex 1 is the full reply from the Danish Data Protection Agency on companies' responsibility to protect children's data according to the GDPR.

1.3. Danish children and online gaming

According to the survey Children's Playing Habits 2020, 92 percent of the surveyed Danish children aged 1-15 years have tried online gaming, and half of them are gaming on a daily basis. Older children are gaming more than younger children. More boys (28%) than girls (19%) are gaming several times a day, and the group of 9-11-year-olds are gaming the most. The older children are gaming for a longer period of time - most 9-11-year-olds (23%) and 12-15-year-olds (23%) are gaming 2-4 hours the days that are gaming. According to the study, the most commonly used devices for gaming are smartphone and tablet. When looking at gender and age, there are differences in the use of devices. Several boys use console and computer for gaming. Girls prefer smartphone or tablet [10].

Danish children aged 10-12 do not comply with the age limits on online games, shows a study from Telenor 2020 [11] which concludes that even though the age limit on most social media is 13 years, and the age recommendation on most used online games are 12 years, Danish children gain access at an earlier age. This is done with the parents' knowledge, as the majority have approved the children's use of the digital media.

DEFINITION OF DATA ETHICS

Data ethics is about responsible and sustainable use of data. It is about doing the right thing for people and society. Data processes should be designed as sustainable solutions benefitting first and foremost humans. Data ethics is more than mere compliance with legislation. It also refers and adheres to the principles and values on which human rights and personal data protection laws are based. It's about honest and genuine transparency in data management. To actively develop privacy-enhancing products and infrastructures. In short, to treat someone else's personal information in the same way as you would wish your own, or your children's, treated. [9]

The games are, for the most part, funded through advertising technology (ad-tech) - ie. in some cases the children's personal data."

2.0 Digital games and use of data

In 2014, Joe Newman Joseph Jerome and Christopher Hazard[12] wrote in a scientific article[13] that computer games: *"collect and generate enormous amounts of information about their players, much of which may be considered highly sensitive. This data includes information relating to the real world, ranging from a player's voice or physical appearance to his location or social network. It also includes detailed information from the player's actions within the game world, which may be analyzed to create in-depth profiles of a player's cognitive abilities and personality. Information collected within a game has many uses both within and outside the gaming ecosystem".*

Data is the fuel of artificial intelligence. Every single data point that players generate by interacting with each other and with the game can be analysed by a gaming platform through algorithms. This can continue to make the game even more entertaining and immersive, which again helps increase the user base.

But many out-of-game actors have massive interests in the data as well. Assistant Professor of Media Studies, David Nieborg,[14] from the University of Toronto, who conducts research in gaming and platform economy, says in this context that: *"people should be worried. The intricacies of gameplay data can tell you a lot about what makes people tick, and what's going on with them — studies have shown that you play games differently when you're depressed, or dieting. Nobody gets too upset about games, but the underlying technology is really powerful. These people are really pushing the technology to the limits where the potential for abuse is massive"*[15].

2.1. Microtargeting

Data from games can be used in analyses, for example to predict "player type" based on psychology. In a patent from 2007[16], Google describes a technology that uses surveillance of users' interests and gaming activity to promote micro-targeting of advertisements:
"Information about a person's interests and gaming behavior may be determined by monitoring their online gaming activities (and perhaps making inferences from such activities). Such information may be used to improve ad targeting. For example, such information may be used to target ads to be rendered in a video game being played by the person".

The patent description also suggests monitoring chatting in the game to reveal personality traits in a player *"e.g., literate or illiterate, profane, blunt, or polite,*

quiet or chatty, etc. Also, user play may be used to characterize the user (e.g., cautious, strategic, risk-taker, aggressive, non-confrontational, stealthy, honest, dishonest, cooperative, uncooperative, etc.)".

Software codes that monitor how the user moves in the game, what skins the user prefers, what weapons the user uses, how they are used and what conversations the user has with others in the game can be returned to the central server, where they are dissected and used to serve extremely precise advertising on the player's screen. Now, 13 years after Google's patent, the ecosystem of gametech actors has expanded considerably and is much more complex and opaque. As the magazine TechCrunch describes[17], this is partly because the natural home of the F2P business model is mobile platforms, and the first smartphone entered the market in the same year as Google's patent was published.

2.2. Business models

Google is only one of the actors behind gaming, which is currently the most lucrative entertainment industry in the world[18].

The moment a child opens their favourite game, without knowing it they come into contact with a number of actors within a complex system of companies operating within computer game technologies (gametech) that are often intrinsically linked to advertising technology (adtech). This is because by far the majority of online games are free at first. This business model is called Free2Play (F2P) or Freemium.

Most games generate an income through advertising technology that collects and analyses data about players and uses advertising as a source of income and a strategy to attract new users. So, as in many other digital services, the user is the product when something is 'free'.

ACHIEVERS

EXPLORERS

SOCIALIZERS

KILLERS

Industry's wish to identify behavioural patterns and predict player personalities is not new. In 1996, British author, professor and game researcher Richard Bartle suggested that players could be categorised into a spectrum of four different types:

"achievers",
"explorers",
"socializers"
and "killers".

Bartle's theory was eventually adapted to a psychological test that is still used by the industry to understand different types of player psychology.

Microtransactions or in-app purchases are also income-generating. Nieborg writes in his article from 2017 that there is a growing divide between two classes of F2P publishers. The largest group, which he calls "the 99%" consists of app developers that rely on advertising as a source of income. The other very select group primarily relies on in-app purchases as a source of income:

"By far the largest group (let's call them "The 99%") consists of app developers that serve as ad publishers and rely on advertising as a source of income. Then there is the very select group of "Net Advertisers": well-capitalized start-ups, superstar game publishers and studios that rely primarily on in-app-purchases as a source of income and have the know-how and monetary capital to engage in user acquisition campaigns of a mass, often global scale". [19]

The F2P hit-games Clash of Clans and Fortnite are good examples of games that generate substantial revenue through the sale of virtual currency and game items. But this does not mean that they do not also collect massive amounts of data (see page 22 about Fortnite).

2.3. The ecosystem

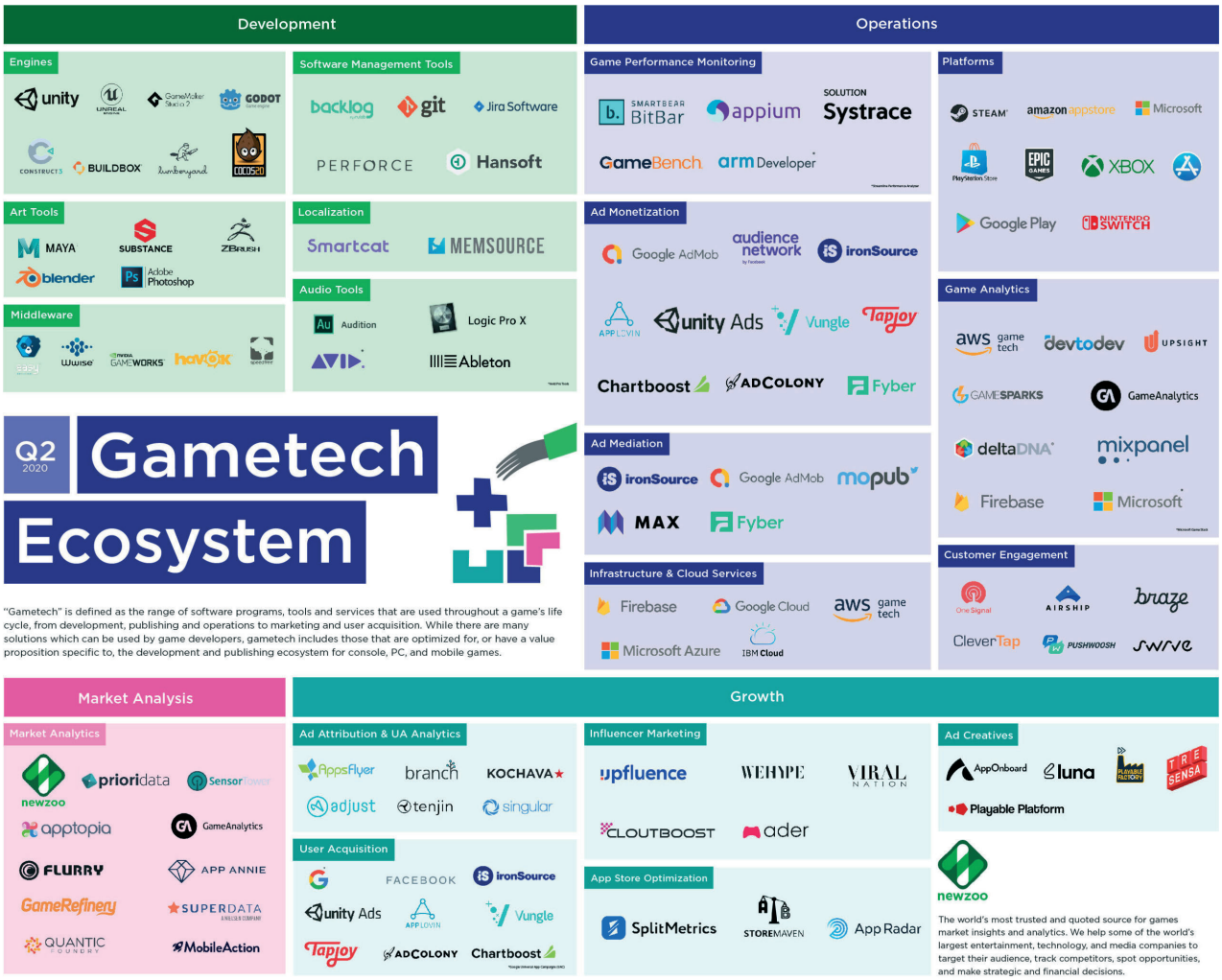
Data collection has been important ever since computer games went online. Today, data collection, data analysis, advertising and online games are intrinsically linked, and there is a plethora of actors in the gametech ecosystem, which the gaming market analysis company NewZoo divides into four main categories:

1) Development,
2) Operations,
3) Market analysis,
4) Growth.

The table below provides a picture of the extent of the ecosystem, but it does not illustrate the fact that some companies are so large that they actually dominate the industry. These are companies such as Google and Facebook as well as Unity and Unreal. Below is a description of some of the actors in the ecosystem.

2.3.1. Game development companies

Game development companies are not even part of the table, but they design the games and enter into contracts with a large number of third parties, including several adtech companies, partly to make the game work and partly to make money on the product. Game development companies have a major responsibility in that they have direct contact with the consumer. But other actors outside the game can embed software codes such that when a user opens the game, data is not only sent to the publisher, but also to several third parties.



Source: https://newzoo.com/insights/infographics/gametech-ecosystem-map-technology-game-creation-supply-chain/

A large-scale study by the Norwegian Consumer Council on nearly 1 million mobile apps found that each app sends data to 10 third parties on average [20]. An example of this is the world's first mobile game success, Angry Birds, published by the Finnish gaming company Rovio. In 2019, Rovio had deals with 43 data controllers and processors, including 14 advertising intermediaries. However, as the author of a critical article in Vox Magazine writes, it is not always certain that the game development company knows exactly what data is being collected about the players: *"To some extent, Rovio and its peers may not even know exactly what they're collecting about their users or how the data is being exploited, thanks to the way software has evolved in the smartphone era. Mobile games are full of other companies' code, a more efficient way of creating something cheap and functional and cute than building it from scratch"* [21].

Game development companies should read through the terms of service from these third-party software providers and assess whether these are compatible

with the development companies' own terms of service, because the developer's product is basically absorbing these third-party providers – and this amalgamation is the real terms of service faced by the user. "But nobody does that", says Joel Reardon, a security researcher at the University of Calgary.[22] However, we would like to emphasise LEGO as an exception in this context, see The Child Data Violators survey by DataEthics[23].

According to the Norwegian Consumer Council, in many cases, third parties transmit user data to further providers in addition to the data already embedded by the publisher.[24]

2.3.2. The game engine

All games need a game engine to be able to work. But what is a game engine? *"When you download a game as an app, only half of the app may have been developed specifically for this game. The rest is code and systems that can be reused from game to game, and this is what we call the game engine"*[25], says Peter Andreasen, a senior software developer at Unity Technologies to dr.dk. Unity makes the parts work together: *"It's no good if the physics engine says that a box needs to fall down from the table and the graphics engine cannot draw this, and the sound engine cannot play the sound of it. That's why it's important that all the parts work together"*.

Unity was originally a Danish company and is one of the fastest growing companies ever. According to the CEO of Unity Technologies, John Riccitiello, Unity holds around half of the market: "We have different market shares, depending on the platform. But more than half of all mobile games are built in Unity. More than 60 to 70 percent – depending on the platform – of everything built for machines for virtual reality or augmented reality or any of the XR platforms are built in Unity"[26].

Computerworld writes that the Unity engine is used to build at least half of the 1,000 most popular games in App Store and Google Play. The company was established in Copenhagen in 2004 under the name Over the Edge Entertainment, and changed its name to Unity in 2009, when it received a USD 5.5 million capital injection from Sequoia Capital and moved to the US. In September 2020, the Danish-founded gaming company entered the US stock market with a market value of DKK 125 billion[27].

Unity's biggest competitor is the 'Unreal' motor from Epic Games. Epic Games develops the popular game, Fortnite. In September 2018, CBInsights concluded that the gaming industry has been built on the backs of these two engines: Unity and Unreal. [28]

In 2019, Unity Technologies acquired the company delta DNA[29] (see table above under "game analytics"). DeltaDNA writes on its website:

LEARN FROM YOUR DATA Uncover all the insights buried in your game data with deltaDNA's data mining, visualizations and reporting tools.[30]

And:

INTERACT WITH YOUR PLAYERS Engage your players as they want to be engaged, on a personal basis, in real time.

In a video on its website[31], deltaDNA talks about all the data to which game developers can gain access – and how it can be used – and says in this connection: *"We even let you connect third party tools (...) to your data. And it's this level of visibility that lets you identify player segments so you can automatically target players, deliver personalized content at precisely the right time. You can alter the game, send messages and offer real time when they are playing or send personal notifications or emails when they are not playing and encourage them back to the game. And this is when having all of your data at one place becomes really powerful".*

So, Unity is a platform within gaming – just like Amazon is within e-commerce – and is therefore an example of how the different groups and companies in the table above do not fit into just a single category. Unity makes money on a number of different services from games being built, to AI, to advertising: *"Monetization of your Unity project through ads is a great way to generate revenue without charging your customers directly. A successful free ad-supported game will bring in many times the asking price of an ad-free game that must be purchased outright"*[32].

2.3.3. Gaming devices

According to Newman, Jerome and Hazard, not only games log information about users. Gaming consoles collect information about what games players choose to play, and about how long and when they play them. Data points are analysed to create "gaming measurements" that are quantitative measurements of the game itself, of what games players choose to play, and of how long and when they play them.

An example is an approved Sony Interactive Entertainment patent[33] from 2020, which describes a technology that allows PlayStation to automatically detect the user's identity by how they hold their game controller. The patent describes a system that uses sensors (such as gyroscopes and accelerometers) to determine

the identity of specific users by how they hold their controller, and thus automatically log them in or out of their profiles when they use it[34].

2.3.4. Actors in advertising

There are several actors within adtech. Facebook and Google Ads have so-called duopoly. They are followed by four other big advertising platforms: ironSource, Unity Ads, AppLovin and Nativex. Together they have: *"fully monetized the explosive growth of the game industry, accommodating 43% of all game apps in the second half of 2019"* (see model below):

These companies allow user data to be used by third and fourth parties. However, as the Norwegian Consumer Council writes, it can be difficult to distinguish between these companies: *"In many cases, the boundaries between these categories of third-party vendors are blurry, meaning that an analytics company may also be selling consumer profiles, or an advertising company could also provide analytics. Unless described in the privacy policy of the app or website, it is difficult to distinguish what kind of service an individual third party is providing in any particular case"*[35].

2.4. Lack of transparency

In a model we have referred to a couple of times above, Newzoo is trying to visualise the network of gametech actors. In reality, these companies are so intertwined that it is difficult, if not impossible, to locate where one phase begins and another one ends. The ecosystem of actors within gaming and advertising technology has a tangled root system, which can seem impossible to untangle. This illustrates that the way in which mobile games collect and share information about their users, and details about the type of information they collect and share are opaque. This leaves the consumer – in this case the child – in a very poor place and vulnerable to manipulation, for example.

Source: https://sp2cdn-idea-global.zingfront.com/report/21b83ae0c8077ed974c729b61c8bc2f4.pdf

3. Advertising and manipulation

3.1 Persuasive game design

Manipulative design is not just about advertising and sale but also about getting the child to spend more time and attention in the game. Because the more time and attention the child spends gaming, the more data it generates. But as already mentioned, it is unclear to children what data are used for. The organization 5Rights, which works to promote children's digital rights both in and outside the UK, puts it this way: "Services that look free, especially to children, are predicated on a service contract paid for with the currency of personal data. The value of this data and the lengths to which the digital environment is designed to gather it are opaque to most users, and nearly all children[36]".

Thus, while data collection and data use are opaque to children, it can have implications for digital services' ability to persuade children to stay longer in their universe. The Disrupted Childhood report highlights how digital services, including online gaming, routinely implement persuasive design features into their products with the specific intent of collecting personal data for commercial use.

An example of such a feature often used in game design is the use of music or sounds that aim to de-sensitize the child to its immediate physical environment. Combined with, for example, sharp intrusive sounds, they can make the child hyper-aware of the screen. Another example is that artificial intelligence based on data can learn when it is best to contact the individual child in order to create re-engagement in the game. The report further states that some games do not allow the child to save the game until it has reached a certain place - that everything the child has previously achieved in the game disappears if it leaves the game. It further mentions that children may be more likely to stop playing if the pace becomes predictable. Furthermore, a built-in barrier that can extend the child's stay in the game may be that a user is forced to consume something in the game before it can move on. It can, for example, be an advertisement that the child has to watch to the end in order to get ahead in the game. There are many more examples.

3.2 Advertising

Children are particularly vulnerable to advertising. Naturally, children's resistance differs on the basis of a number of parameters, including age, but children are generally described as a particularly vulnerable consumer group[37].

Children's critical thinking skills are still immature, and they do not have the same skills as adults to control their impulses. The American Academy of Pediatrics writes that school-aged children and teenagers may be able to recognise advertising but often are not able to resist it when it is embedded

within trusted social networks, encouraged by celebrity influencers, or delivered next to personalized content[38].
Despite this – or perhaps because of this – a comprehensive study from the Department of Computer Science at the University of Oxford[39], of 959,000 apps from the US and UK Google Play stores shows that apps targeted at children are amongst the most worrying users of third party cookies:

- Most apps contain third party tracking, and
- the distribution of trackers is long-tailed with several highly dominant trackers accounting for a large portion of the coverage.

The extent of tracking associated with the individual apps differs between categories of apps. But, according to the study, news apps and apps targeted at children appear to be amongst the worst.

A scientific study from the University of Michigan C.S. Mott Children's Hospital[40] shows that even apps for very young children are full of potentially manipulative advertisements to get them to spend money, for example. An analysis of 135 of the most popular apps for children from the Google Play app store showed that 129 (95%) contained at least one type of advertising. These included use of commercial characters in the game (42%); full-app teasers - encouraging full download (46%); advertising videos interrupting play (e.g. pop-ups [35%] or to unlock play items [16%]); in-app purchases (30%); prompts to rate the app (28%) or share on social media (14%); distracting ads such as banners across the screen (17%) or hidden ads camouflaged as gameplay items (7%). Advertising was significantly more prevalent in free apps (100% vs 88% of paid apps), but occurred at similar rates in apps labelled as "educational" versus other categories.

Josh Golin, the executive director of the Campaign for a Commercial-Free Childhood has called this the first study to systematically explore just how commercialized the preschool app market is. The study examines both how many ads make their way into these apps, and what their advertising strategies are.

In some of the games, children were encouraged to share their progress on social media in the form of buttons or pop-ups – sometimes for a reward in the form of tokens or items. In Candy Crush Saga, for example, the player was asked immediately after opening the app to establish a connection to Facebook to share their progress with friends across devices via a button right below the "Play" button.

In the game My Talking Tom from the Cypriot company Outfit7, a subsidiary of the Chinese chemical company Zhejiang Jinke, a gift fell from the ceiling in the background. The gift looked as if it was part of the game, but when you tapped on it, the player was instead asked to "watch videos and win". In its compre-

hensive report Out of Control, the Norwegian Consumer Council has subsequently examined My Talking Tom 2, which has been downloaded more than 100,000,000 times on Google Play. Among other things, the report concludes that My Talking Tom 2 transmits the user's IP address to Mobfox, Rubicon Project ("The global exchange for advertising") and PubNative ("We build advertising technologies for publishers to maximize their revenues"). In addition to publishing the Talking Tom games, Outfit7 also runs an advertising network that gives access to 350 million active users in 230 countries.

In the game Strawberry Shortcake Bake Shop, players were presented with two tool options: a free standard tool and a locked (in-app purchase) tool. Strawberry Shortcake always indicated how much better the locked tool was. Furthermore, it was more difficult to perform the tasks or operate the game satisfactorily without purchased elements.

Some games were also filled with pop-up ads that interrupted play, and the cancel button was nearly impossible to find. Moreover, several apps used emotionally manipulative tactics, like the way Bubadu's Doctor Kids made its characters cry when children didn't purchase anything from the game. According to the authors, this can be especially deleterious to children because: "Children are known to develop trusting emotional parasocial relationships with media characters and pay more attention to and learn better from familiar characters (...) Games that encourage kids to buy through character encouragement, or discouragement, "may also lead children to feel an emotionally charged need to make purchases" [41].

In a letter to the Federal Trade Commission (FTC), an independent US governmental body to ensure free competition and protect consumers from unfair business practices, the research group from the University of Michigan notes how frustrating it can be when you cannot find a small 'X' to close an ad. Many of the games examined are marketed as being "free" when it is actually often impossible to advance in the game without making in-app purchases. According to the authors, this is deceptive to parents and particularly unfair to children. The main author behind the Michigan study says that: *"Our findings show that the early childhood app market is a Wild West, with a lot of apps appearing more focused on making money than the child's play experience," ... "This has important implications for advertising regulation, the ethics of child app design, as well as how parents discern which children's apps are worth downloading"* [42].

Furthermore, the researchers write that their examples are extra problematic for children because children lack a "meta-awareness" about advertising and, unlike adults, they are unable to critically reflect on their reactions to it. The researchers concluded that the study of 135 of the most popular apps for children showed: *"high rates of mobile advertising through manipulative and disruptive methods"*.

4. Three popular games

4.1. Gaming services disclaim responsibility

More than two years after the General Data Protection Regulation (GDPR) entered into force, children do not seem to enjoy more protection in connection with online games. This is simply because most gaming services disclaim responsibility towards children by requiring users to confirm that they are 13 years old before they use the game. The terms of service on which you click yes to being at least 13 years old, are complete nonsense to many children as well as adults. In 2016, the Norwegian Consumer Council documented that the average consumer often had to read more than 250,000 words of app terms. For most people, this is an impossible task, and therefore they often click the consent button and hurry on without reading the terms. This made Director of Digital Policy Finn Lützow Myrstad conclude that *"the current state of terms and conditions of digital services borders on the absurd. Their scope, length and complexity make it almost impossible to make good and informed decisions"*.

In the following, we will look closer at three popular games. As mentioned in the beginning of this report, it is not possible to make a complete analyses of whether these games are data ethical for children, or whether they comply with legislation. Data ethics in relation to children is a major area which does not have one fixed definition, but data ethics always go beyond legislation. In section 5.2, we recommend that Denmark look towards the UK, which in 2020 implemented a statutory and very detailed Age Appropriate Design Code for services designed for children.

Among many other elements, this code requires that:

- settings must be "high privacy" by default (unless there is a compelling reason not to);
- only the minimum amount of personal data should be collected and retained;
- children's data should not usually be shared;
- geolocation services should be switched off by default.
- Nudge techniques should not be used to encourage children to provide unnecessary personal data, or to weaken or turn off their privacy settings.
- The code also addresses issues of parental control and profiling.

We will investigate three popular games below.

4.2. Fortnite

Facts about Fortnite

- Fortnite was developed by Epic Games, which today has its own store, game engine, developers, etc. and its head office is in the US.
- According to Business of Apps, there were 250 million Fortnite players in March 2019 and apparently 53% were aged 10-25 years [43]. Primary revenues from the game come from microtransactions. According to an analysis from 2019, the vast majority of spending goes on the game currency V-Bucks.
- According to Fortnite's privacy policy, [44] you must be 13 years old to use the service, if you write a younger age, your parents must give their consent.
- Fortnite processes a staggering 92 million events a minute and its data grow by 2 petabytes a month. With every season of Fortnite, Epic Games ingests ever more data from game clients, servers and services [45].
- According to the privacy policy, Fortnite shares personal information with service providers (such as cloud services, here Amazon, email marketing providers and similar), affiliates (such as subsidiaries), marketing partners, Epic Games Store Partners, Epic Account Services and authorities with a court order.

Epic Games was investigated by the British Parliament

A member of parliament (MP) asked Epic Games whether they collect detailed information on how much time players spend playing. The answer was that such data does not exist, to which the MP replied: *"I don't believe that you don't know this information and to me it arouses suspicion that this isn't something you can discuss"*. Another MP asked whether Epic Games made any effort to measure the impact of screen time on players, to which Epic Games' marketing director Matt Weissinger replied: *"Not that I'm aware of"*. Another MP said he was surprised to hear that Epic Games did not ask players to verify their age when installing Fortnite, which has an age rating of 12 years old and upwards [47].

Our conclusion:

We tried signing up to Fortnite via a browser, but were not asked about age. And even though the game asked the user to write their age, it is still possible to lie about your age. Like most other US services, Epic thereby disclaims responsibility that many children use their services and does not seem to do anything active to prevent this. And this is even though much of the content is targeted at children younger than 13 years: something YouTube was fined USD 170 million for in 2019 [46]. Several places describe that Fortnite's F2P business model is based

on in-game purchases, and there are no pop-up ads as in many other mobile games. Because Fortnite shares personal information with service providers, it is impossible for an ordinary user to understand who has access to their data now, and who else could get hold of it through hacks or if the company is sold.

4.3. SUBWAY SURFERS

- Subway Surfers was the most downloaded mobile game from 2010 to 2020 [48], and the most downloaded mobile game in 2020 (figures registered in May 2020) [49].
- The game was developed by SYBO Games whose head office is in Denmark.
- When downloading the game in App Store on an iPhone, the privacy policy states that it takes into account the age the person indicates at the time of download. The policy also states that the game takes into account that sometimes children play, even though it says that the services are not intended for children. When children indicate an age below 13 years, apparently there is no profiling, targeted advertising or geolocation tracking: *"Our Services are not intended to children. SYBO has implemented age-gate to its games to verify players age. Even if you are below the age needed for providing a valid consent for targeted advertising, profiling and geolocation, you can continue accessing our Services. However, there will be no profiling, targeted advertising or geolocation tracking, Our Services will then only contain contextual advertising. We will only collect data, on players under 13 years of age, when it is needed to provide the service and ensure that they are protected in accordance with the applicable privacy laws"* [50].
- So Subway Surfers writes that they only collect data from children in accordance with current legislation and only receive "contextual advertising", which is described by the Norwegian Consumer Council as follows: *"contextual advertising relies on targeting ads based on the content that the consumer is looking at, rather than on the profile of the consumer herself. Therefore, contextual advertising ideally does not rely on the processing of personal data. However, through the use of technologies such as machine learning, contextual advertising can also be used for sophisticated targeting purposes"* [51].

Our test and conclusion:
Even though Subway Surfers, like Fortnite, says that the game is only for users above 13 years, they do not disclaim responsibility in the same way as Fortnite, but recognise that their game is being used by children younger than 13 years, and that the children's data must be protected. According to the terms, children who sign up and indicate that they are younger than 13 years will not be able to sign up using Facebook, for example.

We had a 12-year-old boy download and play Subway Surfers on an iPhone 6 for 30 minutes. He registered the following:

- If he watched a video ad, he could get game items.
- If he watched a video ad, he could survive longer – i.e. he could get an ”extra chance” even though he was actually dead.
- There were loot boxes on the route, and the value of the boxes doubled if he watched a video ad.
- He got coins to use in the game (which he could buy game items for) by watching ads.
- In the shop, he was offered to spend real money on skins or other game items.
- He was exposed to ads for Nerf toy guns, the Cluedo game, instant noodles, etc. On the face of it, it is difficult to see that an instant noodle ad is contextual advertising.
- By watching a video ad, he got keys that he could use to survive in the game.
- He was ”locked inside” an ad for an emoji game that he had to play to get out.
- Several of the ads lasted for 20 seconds, and he could not continue the game without watching some of the ads in full (no possibility to escape).

4.4. CANDY CRUSH SAGA

- Candy Crush Saga was the most downloaded mobile game from 2010 to 2020, with 1.2 billion downloads[52].
- The game was developed by King Digital Entertainment; a Swedish video game developer based in Malta. King was sold to Activision Blizzard in February 2016 for USD 5.9 billion[53].
- When the game is downloaded in App Store on an iPhone, the age limit is set at +4 years. When you open the game, it says: *”We have updated our terms of service. You must confirm that you accept our terms of service and that you have read our privacy policy to continue playing.”* When clicking on the privacy policy and reading under children, it says: *“You must be over a certain age to play our games and use our Services, depending on where you live. For the full list of age restrictions by country, please see below. We do not knowingly collect or solicit personal information from or direct or target interest based advertising to anyone under the ages set out below, or knowingly allow such persons to use our Services.”*[54].
- So they say that you have to be 13 years in Denmark to use the game. Players do not actively have to indicate whether they are older or younger than 13 years, and players are treated in the same way, irrespective of the age they state.
- In a 2018 article, Greg Carroll, director of programmatic advertising at King says: ”King looks to help within the industry by offering to share its first-party data. This, at moment, includes basic demographics and device IDs, but it’s building more-engaged audience profiles also. It says that it offers up as much data as possible because *”we don’t want to be a walled garden”* like Google or Facebook, as it knows that if you try to emulate the big boys *”you’re not going to win”*[55].

Our test and conclusion:
We must assume that the service processes children's data like the data of adults, knowing that many users are children. Through its graphics, the game appeals strongly to young children. The thereby does the same as Fortnite and disclaims responsibility, even though much of the content is targeted at children – something YouTube was fined for in the US in 2019.

We had a 12-year-old boy download and play Candy Crush on an iPhone 6 for 30 minutes. He registered the following:

- He was not exposed to ads.
- He could buy gold bars in the shop.
- He was rewarded with gold bars (which can be used in the shop) when his profile reached a higher level.

5. Conclusion and recommendations

5.1. Conclusion

From the moment a child opens an app or loads a website, collection of data on the child using the game can begin: How often they play and how they play. What location and what device they are playing on etc. However, children should enjoy more protection against data collection and advertising than adults. As a society, we have committed ourselves to this through treaties and legislation. Because data can be hacked, data can be used to reveal children who struggle with bad habits, addiction or who are otherwise vulnerable, and data can also be used to microtarget specific advertising messages to specific individuals in real time, which is unacceptable for children under the age of 13 years, as they are not resistant to manipulation in the same way as adults. However, data generally has many potential uses, and therefore it is important to gain an overview of what actors have what data on what individuals and for how long.

Now, more than two years after the GDPR entered into force, children gaming do not seem to enjoy more protection. Most gaming services disclaim responsibility towards children by requiring that users must be 13 years old to use the game. There are a few exceptions – such as Subway Surfers from the Danish company SYBO – that allow children to state that they are under 13 years, and in this way they can use the game without being tracked and profiled, although they are still exposed to a number of ads.

DataEthics.eu has previously examined LEGO in their report The Child Data Violators[56]

The company, which primarily has users under 13 years, assumes a data ethical responsibility in relation to children. LEGO's point of departure is that their apps are targeted at children, so age verification is not necessary unless data is collected. If the child is to be able to comment, share pictures, etc. in the games, there is a function that requires verification. In the same way, LEGO recognises that parental consent is necessary if the app is for a mixed user group. For apps with older users as well, there are other protective elements. For example: If a child younger than 16 years buys a sword in the game, there will be a restriction on how much money the child can spend. The restrictions become less strict as age increases. Finally, LEGO believes that as a company it has a shared responsibility not to collect and use data about children, even though the children may lie about their age – which the Danish Data Protection Agency also points out – just as a company is responsible for how its subcontractors, including third parties, behave in relation to personal data.

On the basis of this report, we recommend the following:

5.2 Six recommendations

We recommend:

- That Denmark implement a set of standards interpreting and explaining exactly how to apply the GDPR for companies that make money from children using their digital gaming services – even if the services generally state that they are not targeted at children. Such a standard (referred to as The Age Appropriate Design Code) entered into force in the UK in 2020[57]. We recommend that a similar standard be introduced in Denmark.
- That funds be allocated for a technical study on the sharing of children's data on the 20 most popular games used by Danish children.
- That additional resources be allocated for the Danish Data Protection Agency to ensure that consumer watchdogs, such as the Danish Consumer Council and the Danish Data Protection Agency, have sufficient resources to ensure that data protection legislation and other relevant legal protection for children are not only implemented but also complied with - and that those who fail to comply with this are held accountable.
- That a board, independent of the industry and the state, be set up in Denmark, focusing on data ethics, adtech and children. Among other things,

the board should examine the advantages and disadvantages of using new data ethical technologies for age verification. An example of this is the British age verification service, Yoti, which in 2019 was certified as an approved age verification mechanism for age-restricted websites in Germany[58].

- That gaming influencers who stream on digital platforms, such as YouTube and Twitch, make up a separate and fairly commercial ecosystem of gambling and advertising technology in a close symbiosis with other actors in gaming. This ecosystem should be examined in a separate analysis to determine the responsibility of these influencers.
- That the overall topic "children and online gaming" include relevant areas which are not covered in this report, but which require a closer critical review from the government, including:
- The significance of the amount of time spent on sedentary gaming in relation to health factors;
  - The quality of the social interaction on gaming platforms;
  - The significance of loot boxes and ads for gambling addiction among children;
  - The spread of fake news and extremism on gaming-related platforms;
  - Social inclusion and exclusion among children and young people in Denmark related to gaming (both inside and outside the games);
  - Age limits and possibilities of age verification;
  - Grooming and other elements related to child protection;

These elements are all part of a billion-dollar industry that is still growing and should be given much higher priority than today. All that is certain is that the problems will not get smaller as the industry grows bigger.

5.3. Particularly for parents

Parents who give their children under the age of 13 access to games should consider the following:

- Make sure that your children use another name than their own and that they do not give away their address, photos or other information to the game.
- Install a VPN service on your child's computer or mobile devices, and for gaming consoles, install the VPN on the router, or use ExpressVPN, for example, for a PlayStation[59]. Change location regularly, so that your child's real location data cannot be collected by the game.
- If the game is played through a browser, then use a privacy-oriented browser, such as Firefox, to ensure that the settings are set to block third party cookies.
- Talk to your child about the game and keep an eye on what is written about the game online, as there are often warnings against illegal and unethical games.
- Talk to your child about what it means to be a public person: That everything they do in the game is publicly available.

Annex 1

Questions to the Danish Data Protection Agency

1) When the game states that the user must be 13 years and when "the age of digital consent" is 13 – but the game/program does NOT ask the user to indicate their age – is this lawful according to the GDPR?

2) When the game/program states in their policy that the user must be 13 years – and when "the age of digital consent" is 13 – but the child lies about their age (as many children do) to use the game/program (and the game/program thereby reaps data from a user under 13 years), is the game/program acting unlawfully according to the GDPR? In other words: Should the company behind the game/program make sure that it complies with the GDPR and not collect and use data on children under 13 years?

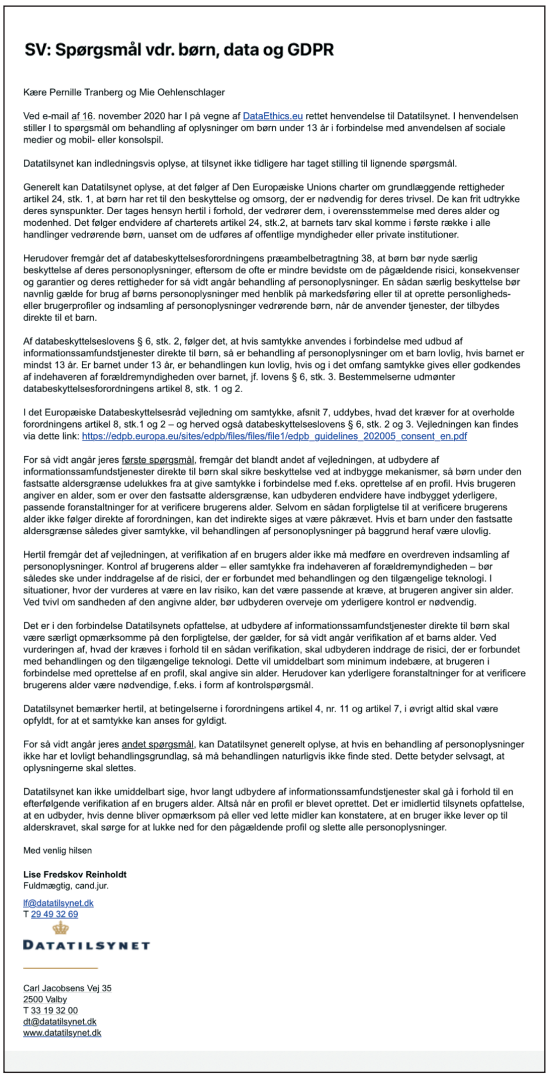
Email from the Danish Data Protection Agency, 27 November 2020

In an email dated 16 November 2020, you contacted the Danish Data Protection Agency on behalf of Dataethics.eu. In your email, you ask two questions about processing of data on children under 13 years of age in connection with use of social media and mobile or console games.

Initially, the Danish Data Protection Agency can state that the Agency has not previously considered similar questions.

Generally, the Danish Data Protection Agency can state that Article 24(1) of the EU Charter of Fundamental Rights states that children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. Moreover, Article 24(2) of the Charter states in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.

In addition, recital no. 38 of the General Data Protection Regulation states that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.



SV: Spørgsmål vdr. børn, data og GDPR

Kære Pernille Tranberg og Mie Oehlenschlager

Ved e-mail af 16. november 2020 har I på vegne af DataEthics.eu rettet henvendelse til Datatilsynet. I henvendelsen stiller I to spørgsmål om behandling af oplysninger om børn under 13 år i forbindelse med anvendelsen af sociale medier og mobil- eller konsolspil.

Datatilsynet kan indledningsvis oplyse, at tilsynet ikke tidligere har taget stilling til lignende spørgsmål.

Generelt kan Datatilsynet oplyse, at det følger af Den Europæiske Unions charter om grundlæggende rettigheder artikel 24, stk. 1, at børn har ret til den beskyttelse og omsorg, der er nødvendig for deres trivsel. De kan frit udtrykke deres synspunkter. Der tages hensyn hertil i forhold, der vedrører dem, i overensstemmelse med deres alder og modenhed. Det følger endvidere af charterets artikel 24, stk.2, at barnets tarv skal komme i første række i alle handlinger vedrørende børn, uanset om de udføres af offentlige myndigheder eller private institutioner.

Herudover fremgår det af databeskyttelsesforordningens præambelbetragtning 38, at børn bør nyde særlig beskyttelse af deres personoplysninger, eftersom de ofte er mindre bevidste om de pågældende risici, konsekvenser og garantier og deres rettigheder for så vidt angår behandling af personoplysninger. En sådan særlig beskyttelse bør navnlig gælde for brug af børns personoplysninger med henblik på markedsføring eller til at oprette personligheds- eller brugerprofiler og indsamling af personoplysninger vedrørende børn, når de anvender tjenester, der tilbydes direkte til et barn.

Af databeskyttelseslovens § 6, stk. 2, følger det, at hvis samtykke anvendes i forbindelse med udbud af informationssamfundstjenester direkte til børn, så er behandling af personoplysninger om et barn lovlig, hvis barnet er mindst 13 år. Er barnet under 13 år, er behandlingen kun lovlig, hvis og i det omfang samtykke gives eller godkendes af indehaveren af forældremyndigheden over barnet, jf. lovens § 6, stk. 3. Bestemmelserne udmønter databeskyttelsesforordningens artikel 8, stk. 1 og 2.

I det Europæiske Databeskyttelsesråd vejledning om samtykke, afsnit 7, uddybes, hvad det kræver for at overholde forordningens artikel 8, stk.1 og 2 – og herved også databeskyttelseslovens § 6, stk. 2 og 3. Vejledningen kan findes via dette link: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

For så vidt angår jeres første spørgsmål, fremgår det blandt andet af vejledningen, at udbydere af informationssamfundstjenester direkte til børn skal sikre beskyttelse ved at indbygge mekanismer, så børn under den fastsatte aldersgrænse udelukkes fra at give samtykke i forbindelse med f.eks. oprettelse af en profil. Hvis brugeren angiver en alder, som er over den fastsatte aldersgrænse, kan udbyderen endvidere have indbygget yderligere, passende foranstaltninger for at verificere brugerens alder. Selvom en sådan forpligtelse til at verificere brugerens alder ikke følger direkte af forordningen, kan det indirekte siges at være påkrævet. Hvis et barn under den fastsatte aldersgrænse således giver samtykke, vil behandlingen af personoplysninger på baggrund heraf være ulovlig.

Hertil fremgår det af vejledningen, at verifikation af en brugers alder ikke må medføre en overdreven indsamling af personoplysninger. Kontrol af brugerens alder – eller samtykke fra indehaveren af forældremyndigheden – bør således ske under inddragelse af de risici, der er forbundet med behandlingen og den tilgængelige teknologi. I situationer, hvor der vurderes at være en lav risiko, kan det være passende at kræve, at brugeren angiver sin alder. Ved tvivl om sandheden af den angivne alder, bør udbyderen overveje om yderligere kontrol er nødvendig.

Det er i den forbindelse Datatilsynets opfattelse, at udbydere af informationssamfundstjenester direkte til børn skal være særligt opmærksomme på den forpligtelse, der gælder, for så vidt angår verifikation af et barns alder. Ved vurderingen af, hvad der kræves i forhold til en sådan verifikation, skal udbyderen inddrage de risici, der er forbundet med behandlingen og den tilgængelige teknologi. Dette vil umiddelbart som minimum indebære, at brugeren i forbindelse med oprettelse af en profil, skal angive sin alder. Herudover kan yderligere foranstaltninger for at verificere brugerens alder være nødvendige, f.eks. i form af kontrolspørgsmål.

Datatilsynet bemærker hertil, at betingelserne i forordningens artikel 4, nr. 11 og artikel 7, i øvrigt altid skal være opfyldt, for at et samtykke kan anses for gyldigt.

For så vidt angår jeres andet spørgsmål, kan Datatilsynet generelt oplyse, at hvis en behandling af personoplysninger ikke har et lovligt behandlingsgrundlag, så må behandlingen naturligvis ikke finde sted. Dette betyder selvsagt, at oplysningerne skal slettes.

Datatilsynet kan ikke umiddelbart sige, hvor langt udbydere af informationssamfundstjenester skal gå i forhold til en efterfølgende verifikation af en brugers alder. Altså når en profil er blevet oprettet. Det er imidlertid tilsynets opfattelse, at en udbyder, hvis denne bliver opmærksom på eller ved lette midler kan konstatere, at en bruger ikke lever op til aldersskravet, skal sørge for at lukke ned for den pågældende profil og slette alle personoplysninger.

Med venlig hilsen

Lise Fredskov Reinholdt
Fuldmægtig, cand.jur.

lf@datatilsynet.dk
T 29 49 32 69

DATATILSYNET

Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
www.datatilsynet.dk

Section 6(2) of the Danish Data Protection Act states that if consent is applied in connection with the offering of information society services directly to children, the processing of personal data concerning a child is lawful, provided the child is no younger than 13. If the child is under 13, the processing is only lawful if and to the extent that consent is given or approved by the holder of parental responsibility for the child, see section 6(3) of the Act. These provisions implement Article 8(1) and (2) of the General Data Protection Regulation.

Paragraph 7 of the European Data Protection Board's guidelines on consent elaborates on what it takes to comply with Article 8(1) and (2) of the Regulation – and thereby also section 6(2) and (3) of the Danish Data Protection Act. The guidelines are available via this link: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

As regards your first question, the guidelines state, among other things, that providers of information society services directly to a child must ensure protection by embedding mechanisms so that children younger than the set age limit are excluded from giving consent, for example in connection with creating a user profile. Moreover, if the user indicates an age above the set age limit, the provider may have embedded further, appropriate measures to verify the user's age. Even though such an obligation to verify the user's age does not follow directly from the GDPR, it is required indirectly. So, if a child below the set age limit gives consent, processing of personal data on this basis will be unlawful.

In addition, the guidelines state that verification of a user's age may not lead to excessive collection of personal data. Verification of the user's age – or consent from the holder of parental responsibility – should therefore consider the risks inherent in the processing and the available technology. In situations where there is a low risk, it may be appropriate to require users to indicate their age. If doubts arise about the truth of the age indicated, the provider should consider whether additional checks are required.

In this connection, the Danish Data Protection Agency is of the opinion that providers of information society services directly to children must pay particular attention to the obligation to verify a child's age. When assessing what is required for such verification, the provider must consider the risks inherent in the processing and the available technology. As a minimum, this will entail that a user indicates their age when creating a profile. Moreover, additional measures to verify a user's age may be necessary, for example in the form of control questions.

In this context, the Data Protection Agency notes that the conditions laid down in Article 4(11) and Article 7 of the GDPR must otherwise always be met in order for a consent to be considered valid.

As regards your second question, the Data Protection Agency can generally state that if processing of personal data does not have a legal basis for processing, clearly it may not take place. Naturally, this means that the data must be deleted.

On the face of it, the Danish Data Protection Agency cannot say how far providers of information society services must go in terms of subsequent verification of a user's age. That is after a profile has been created. However, the Agency is of the opinion that, if a provider becomes aware, or through simple measures can ascertain, that a user does not meet the age requirement, the provider must make sure that the relevant profile is closed and delete all personal data.

DATAETHICS

Endnotes

1 https://www.reuters.com/article/esports-business-gaming-revenues-idUSFLM8jkJMI

2 https://www.reuters.com/article/esports-business-gaming-revenues-idUSFLM8jkJMI

3 https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf

4 https://www.theguardian.com/technology/2015/mar/23/twitch-boss-calls-the-end-of-games-consoles

5 Article 31: 1. States Parties recognize the right of the child to rest and leisure, to engage in play and recreational activities appropriate to the age of the child and to participate freely in cultural life and the arts. 2. States Parties shall respect and promote the right of the child to participate fully in cultural and artistic life and shall encourage the provision of appropriate and equal opportunities for cultural, artistic, recreational and leisure activity.

6 https://menneskeret.dk/sites/menneskeret.dk/files/media/researchpublications/downloads/barn_3-4_2019_temanummer_bornekonventionen_0.pdf

7 https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf

8 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en

9 https://dataethics.eu/wp-content/uploads/Dataetik-dk.pdf

10 https://www.medieraadet.dk/files/docs/2021-02/Børns_spillevaner_2020_rapport_1.pdf

11 https://www.mynewsdesk.com/dk/telenor/pressreleases/danske-boern-overholder-ikke-aldersgraenser-paa-digitale-medier-3034565.

12 Joe Newman later worked for gamecompany Electronic Arts, Joseph Jerome founded Centre for Democracy and Technology and Christopher Hazard is from AI-company Diveplane.

13 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483426

14 Vi interviewede David Nieborg 9. november 2020

15 https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush

16 http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220070072676%22.PGNR.&OS=DN/20070072676&RS=DN/20070072676

17 https://techcrunch.com/2019/01/18/free-to-play-games-rule-the-entertainment-world-with-88-billion-in-revenue/

18 https://www.statista.com/chart/22392/global-revenue-of-selected-entertainment-industry-sectors/

19 Nieborg, David B. 2017. “App Advertising: The Rise of the Player Commodity.” In Explorations in Critical Studies of Advertising, edited by Jay F. Hamilton, Robert Bodle & Ezequiel Korin. New York, NY: Routledge, pp. 28-41.

20 https://taenk.dk/sites/default/files/2020-01-14%20Out%20of%20Control%20Final%20version.pdf

21 https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush

22 Ibid.

23 https://dataethics.eu/da/2-ud-af-14-boernetjenester-er-dataetiske/

24 https://taenk.dk/sites/default/files/2020-01-14%20Out%20of%20Control%20Final%20version.pdf

25 https://www.dr.dk/nyheder/viden/teknologi/halvdelen-af-alle-mobilspil-i-verden-bruger-danske-unity

26 https://techcrunch.com/2018/09/05/unity-ceo-says-half-of-all-games-are-built-on-unity/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMlkn2Y5BA4DxkmnSNp64fYUrk-DQNN4G7nkLGMbTz-I8koHtRWCWTRpTuQaIKgQ5Catd-6jZYNWg1je3POu-K8nflGA-ULUHIKD2iLTrP-R0vw29OZaf-9HqZdFNzghkl6c9rVk0DhQbkltLK76nT0eCctnGVduZeL1To-0nLoPUY

27 https://www.computerworld.dk/art/253461/danske-unity-bragede-ind-paa-boersen-i-new-york-med-kaempestigning

28 https://www.cbinsights.com/research/game-engines-growth-expert-intelligence/

29 https://unity.com/our-company/newsroom/unity-technologies-acquires-deltadna-games-liveops-provider

30 https://deltadna.com

31 https://deltadna.com/analytics/

32 https://learn.unity.com/tutorial/getting-started-with-unity-monetization

33 https://pdfaiw.uspto.gov/.aiw?PageNum=0&docid=20200261803&IDKey=5C9780EF136E&HomeUrl=http%3A%2F%2Fappft.uspto.gov%2Fnetacgi%2Fnph-Parser%3FSect1%3DPTO1%2526Sect2%3DHITOFF%2526d%3DPG01%2526p%3D1%2526u%3D%2Fnetahtml%2FPTO%2Fsrchnum.html%2526r%3D1%2526f%3DG%2526l%3D50%2526s1%3D20200261803.PGNR.%2526OS%3D%2526RS%3D

34 https://www.videogameschronicle.com/news/new-playstation-tech-can-detect-users-by-how-they-hold-their-controller/

35 https://taenk.dk/sites/default/files/2020-01-14%20Out%20of%20Control%20Final%20version.pdf

36 https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf

37 https://www.forbrugerombudsmanden.dk/media/49128/born-unge-vejledning-markedsforing.pdf

38 Radesky J. Chassiakos Yb(LR, Ameenuddin N. et al. AAP COUNCIL ON COMMUNICATION AND MEDIA. Digital Advertisement to children. Pediatrics. 2020; 146 (1): e20201681

39 https://arxiv.org/pdf/1804.03603.pdf

40 Advertisig in Young Children's Apps: A content Analysis, Marisa Meyer,* Victoria Adkins, MSW,† Nalingna Yuan, MS,* Heidi M. Weeks, PhD, Yung-Ju Chang, PhD,Jenny Radesky, MD*, (J Dev Behav Pediatr 40:32–39, 2019)

41 https://www.vox.com/the-goods/2018/10/30/18044678/kids-apps-gaming-manipulative-ads-ftc

42 https://www.sciencedaily.com/releases/2018/10/181030091452.htm

43 https://www.businessofapps.com/data/fortnite-statistics/

44 https://www.epicgames.com/site/en-US/privacypolicy

45 https://www.zdnet.com/article/how-fortnite-approaches-analytics-cloud-to-analyze-petabytes-of-game-data/

46 https://kidscreen.com/2019/09/04/youtube-to-pay-us170-million-fine/

47 https://www.bbc.com/news/technology-48692387

48 https://www.businessinsider.com/most-downloaded-games-of-decade-subway-surfers-to-fruit-ninja-2019-12?r=US&IR=T#1-finally-subway-surfers-was-the-most-downloaded-mobile-game-of-the-decade-with-15-billion-downloads-the-game-was-so-popular-that-developer-sybo-games-even-launched-an-animated-series-based-on-the-game-10

49 https://sensortower.com/blog/top-mobile-games-worldwide-may-2020-by-downloads

50 https://sybogames.com/privacy-policy/

51 https://taenk.dk/sites/default/files/2020-01-14%20Out%20of%20Control%20Final%20version.pdf

52 https://www.businessinsider.com/most-downloaded-games-of-decade-subway-surfers-to-fruit-ninja-2019-12?r=US&IR=T#2-an-easy-concept-and-random-rewards-kept-players-coming-back-to-candy-crush-saga-which-has-12-billion-downloads-9

53 https://www.cnbc.com/2019/11/26/kings-riccardo-zacconi-says-facebook-nearly-crushed-his-company.html

54 https://king.com/da/privacyPolicy

55 https://mobilemarketingmagazine.com/king-in-game-advertising-programmatic-rewarded-video-activision-blizzard

56 https://dataethics.eu/da/2-ud-af-14-boernetjenester-er-dataetiske/

57 https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

58 https://mobileidworld.com/yoti-approved-online-age-verification-germany-052906/

59 https://www.expressvpn.com/vpn-software/vpn-playstation

Colophon
First edition, March 2021
Published by: IDA and DataEthics.eu
Author: Mie Oehlenschlager
Editor: Pernille Tranberg
Front page photo: Jessica Lewis, Unsplash