Privacy Protection of Children in Cyberspace_ Compliance with GDPR Regulations

باسم محمد سعد مصطفى [1]
bassemgabr2012@gmail.com

1. Abstract

Currently, the application of GDPR in the children's game industry is recognized as a pragmatic choice. The GDPR has specific provisions about the processing of personal data concerning children and related matters but also faces many challenges in real-life social implementation. Now children's game enterprises do not have mature compliance systems and self-protection awareness needs to be fostered. Besides, there are still many different opinions on whether to implement more compliant processes and system practices than those required by the GDPR. These findings have practical implications for the child game industry and policy implications related to business environment data protection.

Methods: In this study, we reviewed a master dissertation together with compliance statements from operators running children's games; followed by conducting deep interviews among four operators aiming at investigating the process of implementation while reflecting on enterprise self-compliance.

1 –باحث دكتوراه – الهيئة العامة للاستثمار والمناطق الحرة

Background: The new communication technology revelations and popularizations are altering human communications like never before seen; simultaneously bringing unprecedented levels convenience to mankind as well as thrilling adventures that have come along with them which are posing some of the gravest privacy threats ever recorded in history especially among minors who are most vulnerable groups within society should be protected; however European Union General Data Protection Regulation has become a common law basis for protection of individuals regarding their personal data being processed designed to ensure harmonized application throughout states parties adopted it into their national legal systems thus making it applicable universally as such being treated mainstream international instrument that can be relied upon so far by majority countries worldwide including those whose level development may not match up with others which primarily focuses on adults while neglecting such areas like kids' gaming where this remains relatively unexplored territory hence my main aim here is find out how these operators apply GDPR while dealing with children issues.

2. Introduction

These experimental or hazardous activities expose them to great dangers such as drugs accessibility; sexual scenes exposure leading to harassment among peers thereby resulting into social withdrawal even though sometimes they may suffer mental health disorders commonly associated with addiction tendencies but not limited too. Nevertheless, paragraph one of Article 8 from Convention on Rights Child stipulates that “States Parties undertake to respect rights recognized therein and ensure child has been protected against all forms of negligence whether by themselves or through any other person under their care custody control” however given nature complex dynamics surrounding facts it might miss certain points regarding problems associated with newness as well significance thus unable cope up fast enough.

The world’s attention was recently grabbed by the need of safeguarding children while in cyberspace, but it is still evident that more actions should be taken at national and regional levels. The socio-demographic disadvantageousness and educational environment around them does not give what has been demanded as a minimum for them by the Convention on the Rights of a Child. Over 70% of European children are online before they turn 10 years old; within eighteen months, one quarter of kids aged nine through twelve will use social networks actively, with nearly half using some form of social media. The survey also found out that twelve percent of EU residents between ages nine and sixteen had tried gambling over the internet.

3. Key Concepts in GDPR and Children's Privacy

* Consent

Consent (Art. 4(11)) also changes under GDPR framework. While there are other types of consent which may be met, please refer to Art6 for further reading into this topic.

This is specifically important regarding what counts as parental consent, especially when it comes to cases involving kids. Even though GDPR introduces parental consent differently from minors such as age verification on entrance or opting in/out certain data use through internet browsing, legal guardians should remind companies about these exceptions. Finally, if requested data subjects could withdraw their consents anytime as provided in Article7 (3) Though it is hard to understand whether someone who is below eighteen years might fall under exception or not where terms like “appropriate” or “manifestly” have been used.

* Data subject

A data subject (Art. 4(1)) always refers to an internet user within this context. For example, companies cooperating on sharing data may fail at this point. Secondly these details are viewed proportionally. One might gather additional information (Art4(9)). However, GDPR does not say clearly when should we take details collected by means of an internet toolbar or cookies generally gotten from any internet user (Art4(11)).

3.1 General Data Protection Regulation (GDPR) Overview

According to GDPR, a child is an individual under the age of sixteen years (state which exited lowered liability for controller up to thirteen years). However, it recognizes that majority of goods and services targeting kids are really meant for them too, so it tries to ensure that privacy settings, icons, grey crescents and hyper-aware covers are developed in such a way as to hide design from children thereby promoting cyber security. The Regulation and relevant Recital specify that personal expression by child exercising right to access mediated through company website constitutes significant part relating processing personal data Moreover organizations should provide “clear simple language” for any person who happens be child warns against dealing firmly with illegal activities related processing where only adult harmonization notices represent established ability adhere principles fair transparent responsible minimum storage limitation imposed legislative rules shall apply

The General Data Protection Regulation (GDPR) is an EU law on data protection and privacy. The GDPR concerns itself with the rights of individuals to control their personal information, as well as Privacy by Design and Privacy by Default concepts that have long been enshrined in Canadian data protection laws. It was adopted in April 2016, entered into force on May 24, 2016, and became enforceable on May 25, 2018. The GDPR is a uniform regulation across the EU and European Economic Area. Both are a significant improvement over the Data Protection Directive 95/46/EC because they question the limitations of the essence of personal

information, require a mandatory theft notification, and expand the jurisdiction of enforcement authority. Children's privacy also gets special mention under this regulation. While it does not specifically restrict children's data processing activities, nor does it say so directly in each section; however, it does instruct data controllers to implement certain policies for preventing exploitation or misuse of children's privacy. Therefore, having GDPR is a good start even if it doesn't cover everything comprehensively.

3.2 Children's Privacy Rights and Protections

The Commission and Strategy with exclusion from Digital Agenda intend to reinforce parents' and educators' positions particularly regarding need for achieving same level of child protection through traditional means of communication. These levels can only be achieved through technological means that should be provided directly by digital media for being used within safe environments due to current technological advancements.

According to Article 25 of this regulation both at initial design stage system as well as ongoing upgrade/maintenance service must take into account "data protection by design" principle which seeks to ensure higher level safeguarding measures are taken whenever processing information takes place Children's rights should always be reflected upon when designing ICT systems." Where services involve processing personal data especially if done by children then competent authorities ought to pay closer attention towards children's specific requirements while ensuring more visibility for data

subject persons, increased obligations in terms of compliance coupled with reduced risk relating to data protection.

4. Challenges and Risks in Cyberspace to Children's Privacy

* Dangers posed by children using the internet of things

The Internet of Things (IoT) is an internet system that involves the application of common appliances such as wearable gadgets, home-based systems, kitchen devices among others that connect to the internet through ordinary electronic systems and managed devices. With IoT, this information affects all age groups as it flows to each user in terms of product structure or service use. However, irrespective of the aim domestic content or services consumed already in a household serve; it cannot have equal emotional capacities for every age bracket towards being able to tell apart between those good and bad sides of suchlike "hidden" external sourced information flow. This discrepancy becomes most apparent among kids as well as teenagers whose participation within health care delivery systems; trust in basic weight scales; mobile phone apps monitoring heart activities; becoming part of life with mobile devices etcetera continues increasing daily. Child privacy ignorance will bring about systemic, societal and individual vulnerability within IoT since there is no longer social balance due to service distribution shift while still failing protectiveness rights even for majority subgroups.

* Risks and challenges faced by children accessing the internet

In today's world where communication technology and social media can self-regulate over an individual with control functions persons (especially parents) accept support individual access at younger ages into their lives. Cyber bullying, exposure to negative content provision child disorders caused by giving accurate information third parties loss personal financial data leading socio-economic problems negative public attitudes also expected here. However, unlike adults who have strong knowledge base on issues relating to privacy security rights awareness levels among minors remains minimal therefore making them more susceptible cyberbullying activities that may result into loss personal/financial information being stolen from them along other people's accounts which could create hatreds against themselves based on what happened online about them. As for what "cyberspace" implies freedom, unfortunately this brings new confusions among web users where children are particularly concerned. Unfortunately, these days free problems provide an entrance into 'cyberspace' thereby creating destructive tools through which abuse can occur or one can take advantage of unrestricted content with regard to child privacy, it is unfortunate that most people do not know much about risks associated with technological advancements and social changes in relation to 'privacy'.

* Overview

Considering the different knowledge-based services in cyberspace, all age groups can benefit from educational, intellectual, economic and social gains. However, as the ability to evaluate and process the information acquired

varies among different age groups; it is possible that various forms of misuse and misinformation might arise from products and services utilized. The most vulnerable group of users in cyberspace is children. Despite widespread discussion about how much cyber space has benefited young people through its products and services vis-a-vis their lives; there has been very little protection provided against potential risks that may be encountered by these same individuals while online. Privacy remains the key issue when it comes to safeguarding kids.

4.1 Online Data Collection and Profiling

This section looks at gathering data from children's interaction with the internet as well as their growth patterns_. The first part gives definition, scope and principles of collecting data whiles second part looks into signs or characteristics of collection environment together with types of collected data thus enabling us do a short study based on features and concepts involved in collection process then finally third/fourth sections put type within context_ age and limit it to what kind of collections are made thereby allowing for classification or taxonomy tracking technologies that will afford better protection for children's right to privacy when they surf net.

Online activities such as browsing histories may reveal preferences, health status or even hobbies of a child. Negative practices attract some mentally weak kids who may also exhibit aggressive behavior; have low self-esteem among other things like seeing themselves having psychopathologies which is driven by desire behind motives closely linked with ethics for illegal sites

guiding suicide. Children not intending on participating in these actions could still get affected too. Heavy marketing directed at kids creates a big market where consumer pressure from companies gaming since this service does not fetch money paid by children. To achieve unlawful ends personal information beyond privacy limits may be demanded from minors _STATS_ID used identify report generated OSM or other third-party conduct transaction analysis should collect stats without process defined OSM this number could also be global and quite likely to track user because most probably will be proc. But due to some government departments being capricious there lacks evidence about whether registration operations will submit data strictly according to whims thus failing principal fairness when fails highly likely. However, unit's number is different from several phone numbers at front end.

Children are a desirable and vulnerable group on the internet due to their developmental traits. Children are not buyers who pay for services, so it is not necessary to disclose their information. Participation of children in games and educational websites is not heavily regulated. The unauthorized collection of data by websites can also interfere with children’s rights as well as certain aspects of their rights such as respect for family life, protection of personal data, and children’s right itself. Online data collecting and profiling may lead to violations of penal law which causes significant social harm. With big data and machine learning technologies becoming more prevalent day by day, predictive or data analysis on children’s data is increasingly likely.

4.2 Invasive Marketing Practices

To identify potential customers, professional businesses often carry out detailed analyses on data and then extend specific marketing campaigns towards them; this process is called ‘customer segmentation’ being one efficient marketing tool among many others used today. For instance, using financial information (via credit card number) combined with personal details about an individual player – game companies could get information about different players’ purchasing power; price elasticity; usage levels per game option available; win probability at individual level etcetera then have effective strategies for interventions aimed at improving attendance as well gross income in games.. Within invasive marketing activities where there has been no prior explicit consent obtained by an entity from a person before processing his/her personal data the GDPR policy regards such conduct as intrusive advertising or marketing communication.

GDPR recognizes that children deserve specific care when it comes to confidentiality vis-à-vis safeguarding them against misuse/abuse while using their personal information online. The GDPR requires that privacy tools tailored specifically targeting kids be developed so as foster autonomy among them thus enabling wise decision-making abilities within this age bracket. Therefore, any communication including Information directed at or relating to persons under the age of 18 should be treated with minimum standards respecting both child rights principles enshrined under international instruments such as CRC art.12 as well their interest in privacy according to best practices outlined by UNICEF Innocenti Digest No 16 (2008). Every

person who provides services of the information society to a child shall make reasonable efforts in order to verify that such consent is given or authorized by the holder of parental responsibility for the child concerned.

4.3 Cyberbullying and Online Predators

During distress, two long press events on communication and contact details pages can capture sound children are hearing, further communication with children can be done through live media streaming. The transmission's main points or evidence is recorded and stored in secure cloud server using classification and summarization techniques. All data operations are auditable transparently showing detailed access logs like upload, read, share etcetera.

A help center is not enough for victims of online bullying; once an emergency happens any file sharing, website access or message from kids can be recorded and verified. Smart homes should filter all contents including texts or pictures sent by children to their families or individuals against child eavesdropping problems in future which is typical harassment experienced by youngsters today.

It's important that we can stop the criminal process at an earlier stage. Being able to control personal information exposure better protects both children's and online criminals' anonymity, however, the system needs to balance between growing demand for policing and evidence that allows it to provide protection and risk awareness for children.

To abuse or harass children or gain financial benefit through them, online predators or cybercriminals make use of social media platforms like Facebook, Instagram, Twitter; instant messaging apps such as WhatsApp, Viber; email services like Gmail; sections below news articles where users leave comments as well as chat rooms within games they play together. It is necessary for parents to evaluate threats based on their likelihood so that they can give kids training about being aware while using the internet besides setting rules which guide responsible behavior in cyberspace.

If there is an emergency situation like brutal violence against a child by someone known or unknown then this panic button should be recognized by systems which would initiate voice calls between them before giving all records of conversations held over this period either directly to any authorized person entrusted with such responsibility according proximity indicated through geolocation data received from GPS devices installed on phones used during conversation. The ability of any device that has capability sensing its surroundings through sensors coupled with audio processing abilities should enable later detection environment changes followed immediately intrusion prevention restoration capacities.

What must be done is stakeholders coming up with sets tools/mechanisms compliant with GDPR aimed at safeguarding minors against these activities. What this means is that they are not allowed under any circumstances whatsoever to collect sensitive personal data belonging to children unless authorized by their parents or guardians which includes but not limited to full

names, pictures (photos), phone contacts among others showing where one lives Alternatively what can protect them i.e. Establishing Intrusion Detection Systems (IDS) plus Filters within electronic gadgets used by youngsters thereby preventing capturing and transmitting such kind of information.

5. Framework for Protecting the Privacy of Children in Cyberspace

The Best Available System:

In the digital domain, knowledge about children is becoming a valuable resource for an increasing number of actors seeking data-driven innovation to fuel platform-based markets or their own interests. This includes any information generated by minors; hence, this also brings up concerns on moral and ethical limits in its usage. These limits are not only about safeguarding children's privacy but also protecting their personal development processes and identity formations. The task at hand here involves avoiding using kids' personal data to push them towards certain products which might be against their welfare or unwanted by parents. For example, processes that use data to perpetuate gender preferences and stereotypes for marketing purposes or participate in various sharing platforms among different social media communities come readily into mind. The second process is important for a just society while the first may be necessary depending on whether it respects, protects and fulfills every child's right to privacy as stipulated under ECHR (European Convention on Human Rights), CRC (Convention on the Rights of the Child) and OPCRSCCP2011.

Accessing digital data has been identified as one of the most controversial privacy challenges within the digital environment. Parental responsibility over children's personal information processing especially in activities related to children's profiles has been addressed through revised European legislation ensuring personal data respect rights protection for European citizens' privacy security society enhancement regulation. What consists legal frameworks are rules set forth relating with protection of individual persons with regard to processing of his her personal data contained within prescriptions made out from Union law while requirements coming from GDPR apply across electronic services used by businesses establishments organizations providing such service public bodies minors below 16 years since often times internet services require contracts based legal relations AI technology represented algorithms can play significant roles here artificial intelligence technologies represented algorithms greatly help in this context therefore this research provides findings that contribute knowledge showing areas where European GDPR regulations have not been effectively implemented were major difficulties encountered during enforcement

5.1 Provisions of the GDPR with regard to children's data

The primary concern of GDPR is individual rights, particularly those of children, in cyberspace. Thus, according to Article 40(2), controllers are allowed to use online service providers and appropriate educational materials in an online environment that would help them inform minors about possible risks, promote safe and responsible use of such services as well as provide guidance for parents or guardians. The processing referred to in Article 6(1)

(a) may be authorized by the supervisory authority after taking into account criteria set forth in paragraph 2 second sentence namely: (b) following the Data Protection Impact Assessment referred to in Article 35(4). In addition, unit guidelines discussed under paragraph one should include useful advisory bodies and representations for data protection measures aimed at ensuring both quality and quantity of personal data processing which is lawful fair transparent with respect to minors when using online services. In other words, products, services or systems designed for treatment interests of children in cyberspace must comply with principal data protection by design and default.

Besides defining children as persons under 16 years old, the EU GDPR also has specific provisions relating to processing their personal data while they are using internet services. It should be noted that a controller or processor shall obtain parental consent where a child is under the age of 16 years unless this requirement is satisfied Art8(1) dubbed ‘age limit digital consent’ mainly affecting companies concentrating on kids aged between thirteen and fifteen engaged in online business environments including social media platforms like Facebook among others so as not only protect but also educate them hence creating safer experience thus proposing different levels protection depending on age groups considering Irish law could have least thirteen years olds protected even though still within reasonable range suggested by European Data Protection Board EDPB its guidelines on processing various sets lower limits nationally but within limits.

5.2 International Laws and Agreements

However, these enforcing authorities with different jurisdictions and powers are often a firewall protectionist posture trying to satisfy their public interests from the local context by giving relative protection. It is highly debatable on how countries can protect the market of its locality while protecting jurisdiction. As technology advances, the wider applicability of legal frameworks shifts from informational privacy towards values or fundamental rights (e.g., rights to access, rectification and erasure, restriction of processing, not being subject to automated decision-making alone notification personal data breaches etc.). In addition, there may be common themes such as fair use for decided purpose before sharing legally etcetera which could learn about international laws agreements except various forms like data privacy regulations.

Privacy is a big idea in many nations, and this has been realized by different laws at times either directly or indirectly modified. Different countries are implementing various rules worldwide when it comes to business, data privacy and data protection. Various international organizations contributed and made efforts in this area such as the UN, Council of Europe, APEC, ICCPR among others but mostly OECD (Organization for Economic Cooperation and Development). These attempts led eventually to several legal frameworks for safeguarding personal data all over the world's regions; for example, EU with GDPR or US with COPPA (Children's Online Privacy Protection Act) being two major examples of such regulation respectively.

6. Best Practices for Implementing Privacy Protection for Children

Another new aspect of the GDPR concerning contract management is that anyone acting as processors shall not engage another processor without the controller's prior specific or general written authorization. Using a formalized control does not necessarily guarantee minimum compliance to the GDPR, from a contractual point of view in this sector. One of them could be validating the security and privacy used together with regulation authorities; adopting a checklist and adopting a binding self-regulatory code approved by a supervisory authority. All these best practices should aim at creating a new ecosystem where children can freely develop their personality in cyberspace. It is time for Member State supervisory authorities to include in their user instructions an instruction on how to process children's personal data responsibly. Personal attitude towards data processing and privacy will only be strengthened if parents understand what is happening with their kids' information.

One way to make sure that these principles are adhered to is by having data protection professionals, designers, developers jointly assess these applications. Privacy policies must be produced which go beyond mere minimal compliance with the GDPR because rapid technological change shows this to be insufficiently protective of people's rights under the current state of affairs around personal information management systems design (PIMSD). The GDPR has confirmed that privacy by design and default features should have always been part and parcel of any software development process dealing with customer PII or other sensitive material

but knowing there is a rule does not necessarily prevent it from being broken. GDPR compliance hinges on whether privacy rules are explicitly presented in software's privacy policy or whether software respects privacy.

6.1. Age Verification Mechanisms

Many times videos were viewed by kids in restricted mode which hides comments on videos and helps filter out potentially mature content but it isn't 100% accurate in protecting children so one might ask themselves about age verification mechanisms? A significant number of people believe that "Children should be protected from potentially harmful content by the use of age verification mechanisms." Half of them said it's easy to find inappropriate content on YouTube according to a survey. The report was based on films watched by children at least 8 years old, and the culture of abuse does not derive from YouTube but from broader societal ignorance of children. Internet giants and liberal attitudes toward taking care of others. Parents should contribute to protecting their children as well as platforms this is not just liberal politics it is morality.

But is there really a need for age verification? Much has been said about potential physical and mental harm to kids arising out of no age verification systems being put in place. Those who don't want age verification for children argue that it denies them freedom, so they will be more curious about searching the internet which leads them into dangerous areas or that it's not effective in preventing access by minors while some argue that our

products are not designed with kids in mind therefore we shouldn't have an obligation to block adult-oriented material.

As a practical matter, age verification recognizes only three rough levels of age: "above the minimum age of a user," "not above the maximum age of a user," and "not within the expected consumer age which is arriving at pubertal development." In its report on age verification, required by the Digital Economy Act 2017, the Risk Assessment Panel admitted that it would be virtually impossible to determine someone's true age.

On the other hand, many questions are posed by this process called 'age verification': Who can be trusted with this responsibility? To what extent can or should law let others act as gatekeepers to information protected under First Amendment or state constitutional rights? Is there some way in which verifying ages might work as an effective strategy for protecting young people from having their lives ruined by exposure too soon?

Age verification systems are used to check if a person is old enough to access content or services on the basis of their stated date of birth or other factors. These mechanisms also provide filtering options that allow parents and guardians control over what type(s) of website(s) may be accessed by children using shared computers/devices; for example parental controls such as Net Nanny® block inappropriate sites while others like Norton Family monitor activity across different devices through one central hub The underlying principle behind these systems is that they make tasks more

difficult for children (or anyone else who does not fully understand potential negative outcomes).

6.2 Parental Consent and Control

According to GDPR, processing personal data relating to a child shall be lawful where the child is at least 16 years old. If younger than this then processing may only take place if consent has been given by holder/s of parental responsibility for said child; however Member States can choose another suitable higher/lower threshold provided they ensure 'reasonable efforts' are made verify such person's identity being responsible parent/guardian/other authorized representative. Additionally, national law may stipulate that individuals are considered adults once they reach their 16th birthday so long as it does not conflict with other provisions within this regulation. In order to comply with GDPR requirements, controllers should utilize available technology in verifying holder/s of parental responsibility where applicable. Finally, there is nothing preventing a state from establishing additional legal bases for processing under its own domestic legislation even if the parent's rights have been recognized through requirement imposed by EU law as set out above

As for their personal data children should be under special protection. OPC advocates the GDPR approach towards personal data processing of children. The safety of children needs to be assured by taking extra precautions against unauthorized processing of personal data thereby allowing them to explore online and use Internet-based services as well as enjoy other benefits brought

about by widespread positive aspects of the data economy while ensuring this is done in a manner that supports their growth. The GDPR also stipulates that it is necessary to get parental or guardian consent before processing any child's personal information.

6.3. Privacy by Design Principles

The rules do not talk about how many principles there should be, what ratio these should have nor technical steps among others which need compliance from operators since they do not prescribe as such but provide some guidelines only. It's important for companies to know that operationalization levels differ depending on the size or type of business hence nothing works uniformly everywhere and all over the world hence nothing is absolute either. Each organization has its own way of looking at things therefore one has to find what suits best basing on trial error basis with maximum being considered most appropriate depending on circumstances then evaluated upon finding out whether it was successful/failed; However those operators who are well conversant with current laws protecting minors especially those below a certain age bracket where some form strict standards may apply must ensure highest possible safeguards for such individuals among all other categories falling within broad range covered by definition "children" so they have full understanding about what entails this provision through practical application knowledge at their disposal because failure would result into serious consequences like breach which can lead even severe penalties imposed law courts due lack proper measures adopted safeguard rights affected person(s). These actions taken might include adopting suitable

organizational measures too not just technical ones alone besides evaluating various ways through which personal information could be protected completely realizing that some methods will work better than others depending on each case individually (Art Data Protection 24 Par 1 Decree 101/2018).

One of the most important obligations for businesses, particularly when dealing with minors' data, is to comply with privacy by design and default principles provided in Article 25 GDPR. Among the purposes of processing personal data about children, Prof. Helsinbourg identifies that we need to protect legal rights and other legitimate interests of child subjects such as ensuring their physical development; promoting mental health; preventing abuse/neglect/social exclusion etcetera.; not storing information longer than required legally but also acting according lawfulness vis-a-vis parents' behavior towards them or representatives' actions on behalf of these individuals if applicable under any given context – be it national jurisdictions or international frameworks like General Data Protection Regulation (GDPR). Companies providing services through websites must abide by both CCPA (California Consumer Privacy Act) in USA and GDPR wherever applicable since they may not process personal data relating to a child where an operator has reason to know that he/she is below age of consent under relevant laws within said jurisdiction.

7. Technological Solutions for Augmenting Children's Privacy

All stakeholders should strike a balance between policy-making, legislation drafting/building codes/case law enabling environment creation around digital technologies while safeguarding human rights including those related with online privacy. In the current era when economies are increasingly becoming technologically driven there exists no better way of anchoring more robust cyber rights protection than through policy making backed by sound legal frameworks supported on ethical considerations bankrolled by economic incentives nurtured within cultural contexts sanctioned under law for non-compliance thereof which would then lead us towards enacting appropriate technological measures so as to realize this goal even further still we have seen before how various legal instruments were adopted without rolling back too much over time thereby broadening their scope converging them closer together thus equipping European Union with useful instruments capable extending its frontiers vis--vis private spaces created across different countries worldwide particularly those involving kids but not limited thereto only happening cyberspace.

Privacy in cyberspace, especially for kids, can be improved through technological means. These solutions utilize such advancements as data mining, machine learning, natural language processing, and image analysis to extract digital information in bulk or process huge amounts of text, organize it into knowledge systems by digitizing the knowledge contained therein while building new and creative information ecosystems. Also, these innovative ways are effective at ensuring children's online privacy. However,

technology itself has limitations since it is common for current technological solution sets to address challenges of privacy violations from people, organizations, laws or policies.

7.1 Privacy Enhancing Technologies – PETS

Among them is one disadvantage: overspecialization that occurs when a particular lifecycle phase is considered during development may make them fragmented thereby providing limited options which could cause companies concentrate only on their main competences. However there exist few constructions involving many PETS thus leading to concentration either on hiding personal data or on uses of such (collecting; sharing; publishing). The aim of Privacy Enhancing Technologies is safeguarding personal data against possible misuses by other parties hence keeping off unauthorized persons from gaining access to this kind of information as much as reasonably practicable. In this project described below we will discuss how big firms can meet GDPR requirements recommending very crucial solution for minors data collection therefore some cryptographic-related pets provide additional security because they also protect the stored records from being accessed by unauthorized individuals.

Privacy-Enhancing Technologies (PETS) are mechanisms or tools that help hide boundaries around data so that it is not visible to third parties. They can be used at all stages where personal data could be found including when collected; processed; shared; disseminated etcetera between various actors within an ecosystem like internet platforms during their lifetime cycle . In

simpler terms PETS include any system which ensures protection against personally identifiable information (PII) breaches but alone may not be sufficient even though many pets mentioned under GDPR are meant to achieve privacy by design. By their very nature privacy risks are not confined to technology alone and therefore must be addressed holistically with technology forming just one aspect sometimes not even the primary one. The rest of this section describes several types of pets such as encryption; authentication & authorization; pseudonymization; object transfer control and pseudonymity while outlining pros & cons associated with using them so that specific situations where it is recommended to use pets can be identified.

7.2 Blockchain and Decentralized Identity Systems

Even though there are many areas in which blockchain could be used to help with children's digital identification, it is also important to take into account the potential GDPR-related risks. Under the General Data Protection Regulation (GDPR), children should be able to sign up for and use internet-based services that are intended for them without having to get their parents' permission. In this case, the consent of a child requires consent from his or her parent(s) or guardian(s); thus making authorization easier and more secure within a blockchain structure. Nevertheless, because of the fact that blockchain itself is mainly comprised by smart contract written via source code with contract address and doesn't have natural connection with data; it should define access control rules and safe transaction boundary environment on blockchain. Additionally, incomplete and inflexible characteristics of blockchains' "erm" may cause challenges around data authenticity assurance

as well as digital identity legitimacy validation particularly in child data authorization context alongside parental consent due to risk associated with use of blockchains about rights for accessing stored personal information — like decryption, on-chain restrictions, deletion.

Blockchains coupled with decentralized identity systems can enable an immutable beefing up of the digital identity as well as safekeeping of data exchange. Currently over 1 billion people globally lack any form legal identification some whom are children thereby hindering their ability to use financial services among others which then affects their health seeking behavior hence keeping them poor. Digital identities underpinned by blockchain empower individuals so that they own control over it themselves (which means nobody can delete or alter without owner knowledge) where these can be utilized towards gaining entry government establishments; banks; schools etcetera . Decentralized networks built using blockchain technology have also been used speed up checks on identities while at same time scaling this process such that many more verifications happen than before plus storing key information- like vaccination records; birth certificates ; ID cards – for improved quality of life safety kids in poor urban/rural regions or those who travel frequently.

8. Case Studies and Examples of Successful Privacy Measures

There are a lot of great examples in the first category. Many of them are associated with good practices in some EU member states, especially Scandinavia and the United Kingdom. Good European Union practices related to using personal data about children were studied. They concern awareness-raising measures for children and their parents or legal representatives as well as other relevant actors on how to behave in a safe environment, which should be taken into account by all parties involved in processing such data. This implies appropriate selection of keywords and making operability based on age limitations. So this means that effective selection among keywords used to enable private messaging mobile app success, organizing meetings at schools or involvement in initiatives like COPPA (Children's Online Privacy Protection Act) and Safe Harbor offered advice . Control activities include checking child protection settings for platform security implementation, checking protection settings – basics explained 0f child protection... Individualization aims at high relevance so as to protect the child from being bullied or misled online while ensuring that they remain safe online themselves. The provision of high-quality information to users of a service supports its user empowerment. Effective selection among keywords can help young children educate their age offering more targeted direct responses to searches carried out online by them... All kids' activities are improving through overall security measures which provide more targeted direct responses to searches done online focusing on what needs be done regarding safeguarding children who use the internet/online platforms.

This work package presents good practices and models developed/used within the EU for protecting children's privacy in cyberspace, as well as another group representing best tested practice from several Member States . These best practices relate to online environment privacy for children, providing easily understandable information about use of personal data with kids too young understand long terms conditions thus empowering them at every stage while interacting with any interactive element; four operational EU legal acts on data protection have been tested namely Data Protection Directive 1995 (DPD), General Data Protection Regulation 2018(GDPR), Privacy Electronic Communications Regulations 2003(PECR) and e-Privacy Directive implemented in some MS.

8.1 Social Media Platforms

The platforms can inquire about the age but the easiest and most reliable way to control the content is by using algorithms. Algorithms that learn who someone is – their gender and age, continue growing smarter every day. For instance, Microsoft has developed an algorithm with 95% accuracy level which could identify children quickly among a mixed community of both adults and children on social media platforms thus protecting them amidst such context. If platforms could quickly identify the children and add features making their contents visible only to friends or authorized people for safety, then some controversial matters may be solved .

Because children's content is hard for content recognition systems to identify, it is often left out of recognition altogether. YouTube, Twitter,

Facebook, and Instagram all have age limits set around 13 or 14 for children and base their recognition on this condition of age. TikTok is a new exception to this. It has an automatic age recognition system that can make the account private if users identify as under 16; however, after 16 users can change to public accounts. Children cannot make real use decisions, so restrictions need to be placed on changing privacy settings of accounts and taking further measures to protect children's privacy on social media platforms. Platform developers should also create user-friendly interfaces that allow for informed decisions by both children and parents.

8.2. Educational Websites and Apps

Privacy policies and cookie consent banners, like any other website category, also appear but are unlikely read by children in addition to privacy policy jargon being beyond their understanding. To help with this underlying understanding the "Duckysaurus" tool was created by partner "Digital me" from the Erasmus+ supported project "SEGUR@: Safe on the Internet", which is an icon-based personal data protection paradigm. The prototype includes software that teaches children and young people to respect others' personal data when using online tools by respecting their own. For hearing-impaired children, gamma avatars and sign language have been implemented. Children may fill in a familiarization questionnaire using the tool, to identify with individual or collective results, and state ages of admissibility. You may also register to receive news and updates.

In the “iRead” personalization platform manager collects children's interests and book preferences in order to provide personalized content. Minimal limitation of data processing and required consent, if not done appropriately can lead failures both legal security aspects may pose privacy risks: while using cookies may have a legal impact they also pose security risks.

Educational digital content for minors is another specific category where the personal data processing for the purpose of direct marketing in the form of profiling is allowed as an exception, but again it is subject to effective safeguards such as a parent's right to object. Limited information regarding children will be requested, mainly user’s age and interests ,and in certain cases even overestimated age will be used. Prior parental consent will always be required and age-appropriate data given higher protection.

9. Suggestions for Creating Strong Privacy Protections for Kids in Cyberspace

Indeed, compliance with the GDPR law is a daunting task. Especially when processing minors’ personal data, the role of the collecting entity becomes complex. By processing we mean any operation performed on personal data whether by automatic means or not such as collection, recording, organization, structuring, storage, adaptation or alteration. Only this category is covered by the regulation under article 8; conditions applicable to consent of children in relation to information society services. It should be noted that by minors it does not only mean legally an adult 18 years old Leonardo Silva

but also those who are sixteen years old and therefore this protection goes up to eighteenth birthday.

This chapter sought out to find out how best can organizations comply with GDPR so that they may provide strong privacy protection for children in cyberspace. The General Data Protection Regulation was created with big data challenges in mind and aimed at setting standards that will protect not only adults but specifically young vulnerable members of society. It was developed to enhance control over their personal data by individuals ensure private rights relating to same equalize all entities processing personal information rules and correct imbalances between European system vis a vie national supervisory authorities. Moreover, it intends to make better kids' privacy awareness through consent at such a process where even knowing at age eighteen would have been unimaginable attempt by an individual whom this safeguard seeks foster proper development into citizen. Since its inception many organizations handling personal records have had rethink their policies since they keep on changing everyday according adopted rules. An initial approach towards GDPR is recommended revisiting terms and including policy containing approval themselves conditions.

When kids use the internet, parents get anxious about their safety. They worry about strangers who may try to contact children and that their child might give away personal information online. The General Data Protection Regulation (GDPR) was developed to give more protection for children and their privacy among other reasons. This chapter seeks to investigate how well

the GDPR requirements on children's privacy are observed as well as offer some recommendations on implementing them for better results in practice. My thesis was theoretical and relied upon interpretation of European Union legislation (GDPR) together with its references besides existing research works already done in this area but not yet published or peer reviewed by any reputable journal so far.. To put across my points scientifically throughout this chapter I followed a particular structure guided by those research questions established within main body of my study.

9.1 Education and Awareness Raising Campaigns

All players in the industry, civil society organizations as well governments have joint responsibility towards sensitizing kids, parents and caregivers on dangers associated with these connected things. In order to sensitize people about different risks concerning minors while they are online new campaigns for awareness creation were initiated. Some campaigns have introduced what can be called a 'parent' section or initial talk targeted at teachers together with other school staff members which provides useful tips necessary for guiding young individuals through complex digital space. A fresh medium should be made out of traditional educational activities: schools need to demonstrate that also they form digital citizens among children and early adolescents. Therefore it is important that we increase knowledge levels among many people so that least possible harm may come from these potential connections related hazards during their lifetime…

Usually, it is up to the parent or guardian to protect the child's safety online, but there are other roles that have to be played by different bodies. As we work towards promoting digital skills in society, educational institutions have already started shifting their digital education provision trend to a higher level. There should be training on digital literacy in primary and secondary schools. These educators ought to come up with one framework for digital education; this is meant to lay a foundation for an evolving common digital concept that will not only enhance full inclusion of children but promote global citizenship through shared values as well. Some writers demanded mandatory classes on digital theory, basics of the digital image learning, social media network sites, e-discovery gadgets and apps among others. All these should aim at increasing the level of awareness of youths in particular, and at helping them establish their digital footprint.

9.2. Collaboration Among Stakeholders

In modern society within the organization itself government need not display children's private information about labeling them as a particular child nor suggest situations where other children should avoid doing so. The public should try understanding campaign appreciate it change atmosphere through these cine frames; this will make laws its most effective reflection. Any supplier on the market represents corporate responsibility while meeting needs which arise from consumers' demand but they must also be accountable citizens respecting policy rules and obeying law requirements. In relation with companies access rights towards personal information privacy

settings ought to create an environment where businesses take lead role into protecting it while accessing such private data or protective products.

The problem of children's privacy can only be solved if all stakeholders work together. Parliament, Ministry of Women and Family Affairs in each country as a central administrative agency responsible for protecting children's privacy industry including companies related to children's products general public should participate as much possible in activities regarding protection of privacy. The types governments give corporations permission use peoples' personal details need fixing because those are data which can be processed though minimized.

9.3. Regular Audits and Monitoring

Synopsis – In this chapter, we focus on children's data protection which is increasingly becoming necessary in the world today mainly due to technological advancement. We look at how companies collect these data and process them; but most importantly our concern lies with ensuring that products or services based on such information do not exploit or infringe upon kids' privacy because doing so could have far-reaching negative effects on their lives. Additionally, there are also discussions about compliance with GDPR rules as well as regularity of inspections for privacy-protection compliance purposes. Finally, the need for frequent inspection of privacy-protection compliance is discussed to conclude this chapter .

Regular Audits and Monitoring

Together with the policies and strategies one must also monitor and evaluate the results out of them. Monitoring is easier in many cases when data is available, this will be discussed later on, also with real-time monitoring tools present today. Reports from such monitoring should be analyzed for the age group it targets. In case there are changes in law or regulations, then it is good to do an audit so that we confirm if all policies still serve their purpose and where necessary we make amendments.

10. Conclusion

In a world where the internet has become globalized, personal information generated by children digitally within the next few decades will be on a scale never seen before. This creates more disparity between generations because privacy rights for young people today are likely to face new demands, controls and safeguards online very soon. For these reasons, this chapter takes up the introduction paper primarily discovering some extent of impasse of GDPR and first jurisprudence necessitating etiologically advertisements invasive methods having referendum support.

The processing of personal data of children in an information society entails risks as regards their physical, psychological and moral integrity; therefore there is need to promote awareness about children's rights in the information society and build up their resilience against these threats. Safeguarding best interests of child alongside his/her rights is important same way with ensuring high level data protection for any other individuals i.e., democratic

society functioning, participation public sphere etcetera but it becomes even more significant due to specificnesses inherent to minors. Moreover various potentialities could pose considerable danger towards safety or subjective well-being among kids thereby infringing upon number fundamental freedoms enshrined within European international human instruments. As far our understanding goes provisions provided by GDPR rules here are exhaustive only that Privacy by Design plus Default remain ambiguous legal concepts.

References:

- Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). Past, present, and future of face recognition: A review. Electronics1
- Aljeraisy, A., Barati, M., Rana, O., & Perera, C. (2021). Privacy laws and privacy by design schemes for the internet of things: A developer's perspective. ACM Computing Surveys (Csur), 54(5), 1-382
- Briggs, F. (2020). Child protection: A guide for teachers and child care professionals3
- Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. Computers in human behavior, 110, 1063824
- Donovan, S. (2020). 'Sharenting': The forgotten children of the GDPR. Peace Human Rights Governance5
- Finck, M. & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. International Data Privacy Law6
- Hartzog, W. & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. BCL Rev… 7
- Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 1-228

- Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems9
- Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. Journal of Network and Computer Applications, 171, 10280710
- Kuner, C., Bygrave, L., Docksey, C., & Drechsler, L. (2020). The EU general data protection regulation: a commentary11
- Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. Journal of network and computer applications, 166, 102731.
- Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. Big Data & Society, 7(2), 2053951720976680.
- Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. The ethics of information technologies.
- Skowronski, D. S. (2022). Coppa and educational technologies: The need for additional online privacy protections for students. Georgia State University Law Review.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., … & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. hepl.ch

- Sun, P. J. (2020). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications.
- Thapa, C. & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine.
- Van Der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. The International Journal of Children's Rights, 28(4),