TikTok
Compliance with GDPR For Minor Users

MSIS 672 Data Architecture and Management

Professor Majid Dadgar

Group 5

Dec 3, 2020

Table Of Contents

Executive Summary

As far as people know, there is a huge amount of personal data collected and processed in the social media industry. TikTok, the popular short-form mobile video app, is facing more scrutiny over its data privacy policies. Its extreme popularity among teenagers and preteens has caused concern for the privacy of minors. Mobile app tracker reported that TikTok was downloaded 315 million times in the first quarter of 2020 globally, and has now reached more than 2 billion cumulative downloads [10]. TikTok is known to be accused of its lack of sufficient protection for minor users, lack of transparency around information, communication and regulations for subjects to execute their data rights, and around data usage and accessibility for third parties.

Minors do have a right to protect their personal data according to GDPR, even a specific protection if needed. Minors and parents should be clearly informed and have a comprehensive understanding of the consequence when their personal data is collected, processed, and used. TikTok's current design fails to guarantee minor users data protection under GDPR while it processes more sensitive data such as device information, location and user activity.

We analyzed the current challenges TikTok faces about its minor users, and came up with improvements of TikTok's current data architecture regarding minor users' age verification, minors video uploading, the rating/comments process, the choice of audience, and the direct message system. We tailored TOGAF framework compliance with GDPR for TikTok to define the analysis scope, objectives, principles with rationale and implications, and stakeholders; we have demonstrated each improvement in context diagram and level 1 data flows diagram. Our detailed analysis would be explained using IS architecture and DAMA wheel dependencies. We conclude that if TikTok invests in their data architecture to expand their GDPR compliance to support minor users in all markets. This might increase the data management cost in the short run. However, in the long run it will gain unique competitive advantages over other social media apps by providing minors and parents with data transparency and control over their personal data,and proactivity to comply with GDPR and other local and international data regulations. With these advancements, TikTok would be able to collaborate closely with data protection regulators, minors and parents, leading a secure environment for teens in the social media industry. This also helps TikTok to build up a solid data management architecture and generate greater revenue.

GDPR Overview

The General Data Protection Regulation (GDPR) is a European privacy law1 (Regulation 2016/679 of the European Parliament and of the Council of April 27, 20162) that became enforceable on May 25, 2018 [8]. It is intended to comply with data protection laws with the European Union by applying a single data protection law that is binding throughout each EU member state. According to its Article 3.1, the GDPR applies to organizations that are EU based even if the data are being stored or used outside of the EU. Article 3.2 goes even further and

applies the law to organizations that are not in the EU if two conditions are met: the organization offers goods or services to people in the EU, or the organization monitors their online behavior. The GDPR established a series framework regarding security measures, breach notification, data protection impact assessments, international transfers, consent, transparency, profiling, and enforcement.

TikTok - GDPR for Minor in Social network

Before GDPR regulations came into existence, minors were covered by the age-generic data protection provisions since 1995 provided by Directive 95/46/EC with no special focus on the processing of children's data [5]. The newly adopted EU General Data Protection Regulation (2016/679) (hereinafter 'GDPR' or 'Regulation') has significantly changed the *status quo* and rejected the 'age-blind' approach to data subjects. This was a revolutionary and much needed change as in today's digital age children are using social media at even younger age. As of June 2020, 32.5% of Tik Tok users are teenagers. Minors are more vulnerable to particular behavioral characteristics, emotional volatility and impulsiveness compared to adults. All these factors make minors more vulnerable to falling prey of online frauds, stranger danger, data theft, endangering life situations. To provide special protection in the processing of personal data of minors, Article 9 of GDPR has established a parental consent requirement before the offering of 'information society services' directly to children under the age of 16.

We have studied how TikTok has been working towards complying with GDPR to protect their minor user base. We have used TOGAF (ADM specifications) and DAMA framework to build a suggestive data architecture model for TikTok to support their compliance with GDPR in Non EU regions as well.
GDPR provides the following rights over the personal data of minor data subjects [8]-

1. Right to access personal information
2. Right to erasure of personal data and video content
3. Right to restriction of processing
4. Right to rectification of personal data
5. Parental consent and approval rights

TOGAF ADM Analysis

Preliminary Phase

TikTok Organization Context:

TikTok lacks sufficient protection for minors above 13. Our analysis is within the scope of TikTok's minor users between 13-16. We investigated the functions of minor users' age verification, minors video uploading, the rating/comments process, the chosen audience, and the direct message system.

Objective: Define challenges and find corresponding solutions compliance with GDPR

TikTok is charged to illegally collect data from children under 13. It ends up with being charged for $5.7 million and entered into a consent order with the Federal Trade Commission in 2019 [12]. Although TikTok has claimed that it closed those accounts upon request, it did not delete the data associated with the child users. TikTok has continued to fail to both - obtain parents consent before collecting minor's data and delete minor's data upon request.

From our investigation, TikTok has never verified that an adult was actually monitoring the accounts either for children under 13 or minors between 13 to 16. The function of age consent is easily bypassed by filling with a fake date of birth. There is a default setting which public minors' profiles by providing a list of other users within a 50-mile radius [15], which resulted in minors being massaged and solicited by adult strangers.

All the past complaints indicate the same allegations that TikTok is not asking for minor users' permission, or parental permission before using their data in various ways. In addition to data collection, there were also concerns about how the open messaging system allowed any adult to message any minor user.

Suggested Solutions:

1. TikTok should build a privacy compliance program and comply with data governance.
2. TikTok should heighten standard of care ,particularly for minor users to comply with GDPR
3. Protect minors by practicing parental consent verification of video content, direct message, and video comments (to reduce the risk of being exposed to stranger danger)
4. Routinely monitor compliance. Finally, privacy compliance programs are not "set it and forget it" endeavors. A compliance program should have a built-in monitoring so that TikTok can be sure that the privacy controls are well functioning.

Stakeholder Matrix

Stakeholders	Role	GDPR Impact
Minor User	Minor user includes TikTok users aged between 13-16 years	High
Parent User	TikTok provides a platform for parents of the respective minor user to monitor their child's activity	High
Non follower User	Any User who is not a follower of a minor user. Non follower users do not get any notification about new posts or updates from the user she/he is not following.	Medium
Follower User	Any User who is a follower of a minor user. A follower user gets notified whenever there is a new update or post by the minor user whom he/she is following.	Medium
Third Party Apps	TikTok enables integration with third party apps like Plotaverse, PicsArt, Fuse.it etc and they collect users' data	High
Executive Management	Executives include CEO, CIO,CFO,VP who are interested in the successful running of business with upcoming changes	High
Development Team	This team would include programmers, developers, analysts, researchers who directly get involved by working and implementing the changes	High
Internal Content Moderators	Employees of TikTok who manually review the video content if it has been reported for any malcontent. They are authorized to access the content.	High
Security Maintenance Team	This team is responsible for any account, content, activity, privacy issue	High
Regulatory Sectors	SEC, government, IRS, FTC- find out if there is any breach and impose a penalty	Medium
Investors and Shareholders	Bytedance, Oracle, Walmart are some of the big investors of the organization	Medium

Below is the TOGAF ADM data architecture we utilized to comply with TikTok's current data architecture with the GDPR requirements. Our analysis focused on the Preliminary phase and Phase C- IS Architectures.

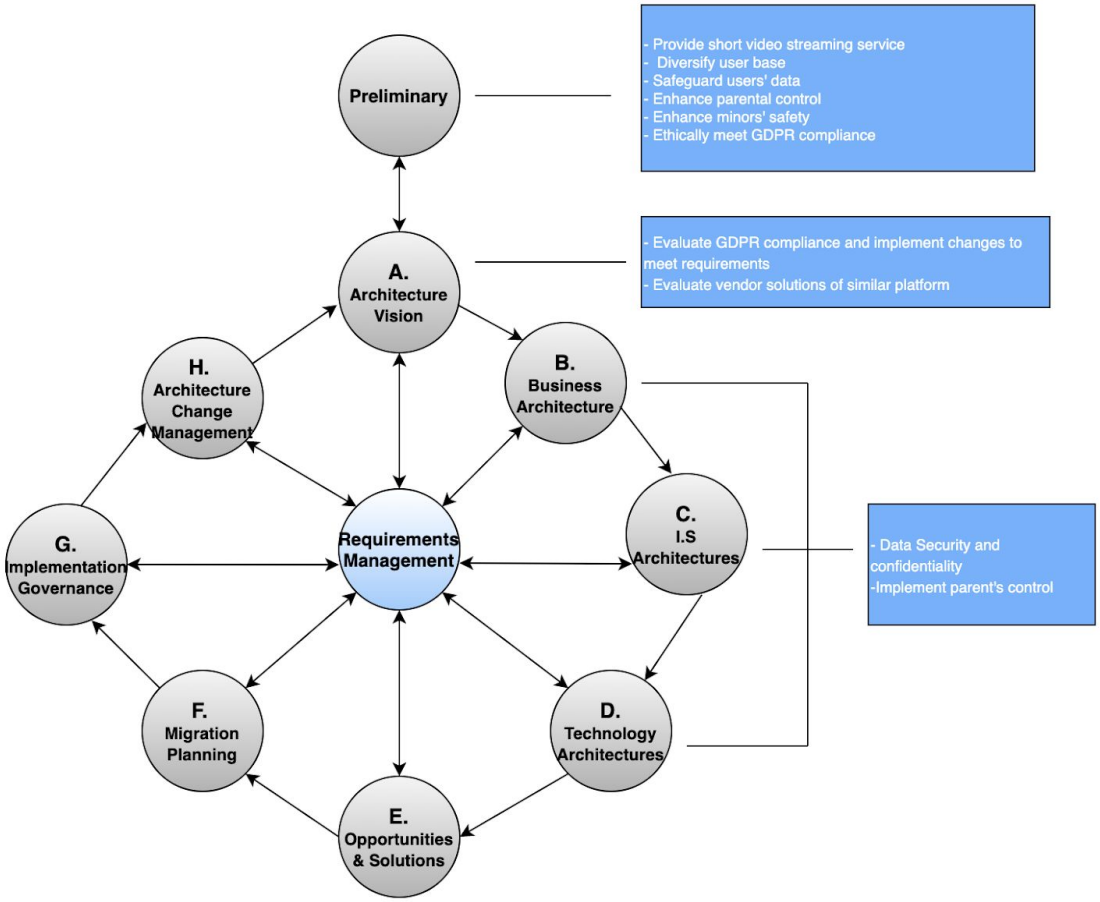

Figure 1: TOGAF framework (scoped for GDPR)

Principles

Principle 1: TikTok will accurately confirm age of user to comply with GDPR

Statement: TikTok must seek parent's approval for minors to verify their age in the registration process.

Rationale: Restricted minors under thirteen could easily set up an account by entering false birth dates. This is the initial step for TikTok to comply with GDPR while the minor in the age of 13-16 uses all TikTok functions. GDPR 8(2) states that "[t]he controller shall make reasonable efforts to verify in such cases [where a child is under the age of consent] that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology [14]."

Implications: TikTok will establish an effective framework for child age verification. TikTok will need minors to fill out the form of parents' contact information. TikTok then will verify parents' information and send them the verification form once the minor inputs their birthdate. By doing so, TikTok is able to prevent underage children from being exposed to age-inappropriate contents such as advergames, sexual content and alcohol-related advertisements.

Principle 2: TikTok will collect and use minor user's data in compliance with GDPR

Statement: TikTok must seek parent's approval to collect and use minor user's data for certain app activity, such as video watches, time in the app, and general usage data.

Rationale: For normal users, TikTok collects certain information automatically from the user's device, including internet or network activities such as device ID, IP address, web browser type and version, country-level location, as well as app usage activity data [14]. In order to comply with GDPR stipulates that "children who have attained the thresh-old age, have the capacity to consent to the processing of their personal data. Concomitantly, children below the threshold age are deemed to lack capacity to consent to the processing of their personal data and an onus is placed on those [14]." TikTok will stop automatically collecting and using minor user's data for certain app activity without parents' content.

Implications: TikTok will post a conspicuous and clearly labelled link (comply with GDPR) to its privacy policy, directly notify parents, obtain verifiable, parental consent before collecting information from children, of the data collection and usage of minor's data.

Principle 3: TikTok will provide extended control or erasure of minor users' personal data to comply with GDPR

Statement: TikTok must take responsibility for deletion requests of minors' data not only from their platform, but also from third party shared platforms.

Rationale: GDPR recital 65 and art. 17 refer to the right of erasure (also referred to as a right to be forgotten) for minor users. "This right embodies the evolving capacities principle by recognizing that as children reach maturity and develop a greater sense of privacy, they may wish to withdraw consent to some previous disclosures of personal information continuing to be avail- able." Since the minors' data shared on TikTok is also accessible via third party platforms,this gives more exposure to their data and when a deletion request is made, TikTok should think about deleting it from all platforms as minors' data and protection are critical.

Implications: After deleting the requested content from TikTok server, TikTok will send a notification request to the third party shared platforms about the deletion request from minor.

Principle 4: TikTok will get approval from holders of parental responsibility of minors before posting their content.

Statement: TikTok must seek parent's approval for minors before posting their content (to make sure that nothing inappropriate or too detailed information of their child is made public, threatening their life in any way.)

Rationale: To prevent minors from posting inappropriate or dangerous content. Research indicates that minors are easily induced by others to post inappropriate videos or photos. Since GDPR empowers parents (art. 8(1) to give or withhold consent to the processing of their children's data (when the child is below the threshold age) reflects the current practice of parents making decisions of their children that are in "the best interests of the child."

Implications: After Machine reviewing of the video content, TikTok will generate a review report and send the review report to the parents, requiring their consent before the minor could upload it.

Phase C: IS architecture-DFD diagrams

Analyzing the current framework and operations of Tik Tok and under certain assumptions, we have constructed a current state data flow diagram of TikTok (shown in Figure 3).

Level 0 Contextual data flow diagram (Figure 2) shows how and what data is flowing in and out between TikTok and its major internal and external stakeholders, on a high level.

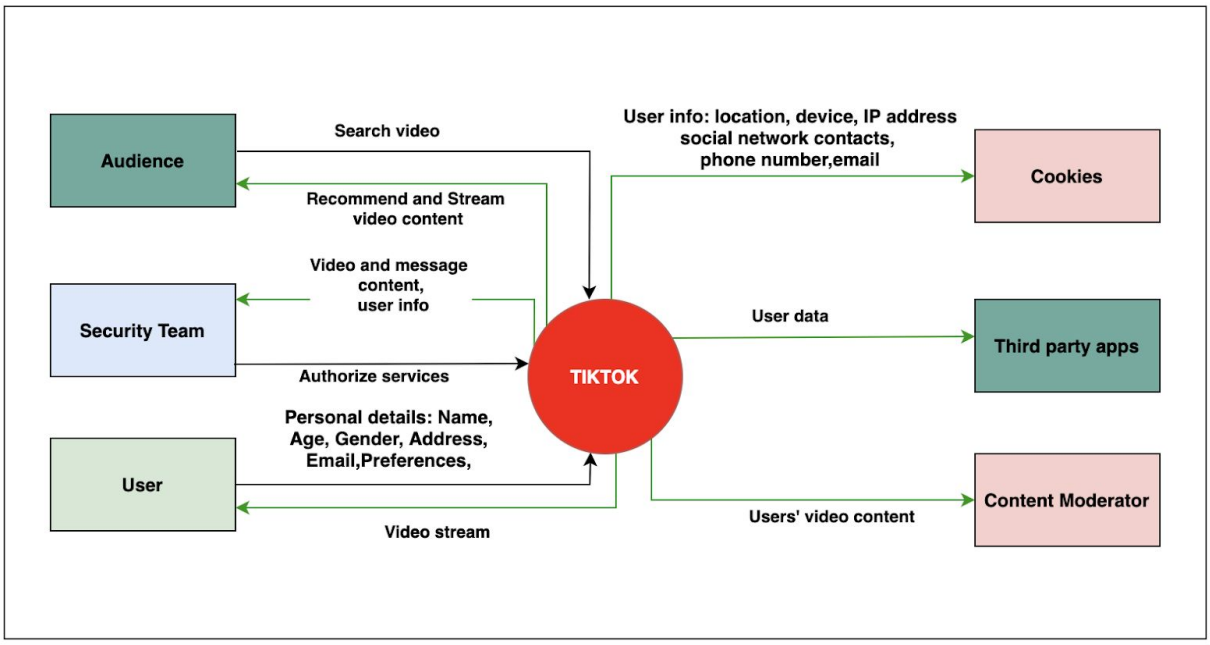

Figure 2 Level 0: Current Contextual Data Flow Diagram between Tikok and major stakeholders

Level 1 (current state data flow diagram) shows how data is flowing and processed within the Tik Tok Information Systems and stakeholders. The diagram shows the current processes related to data handling at Tik Tok.

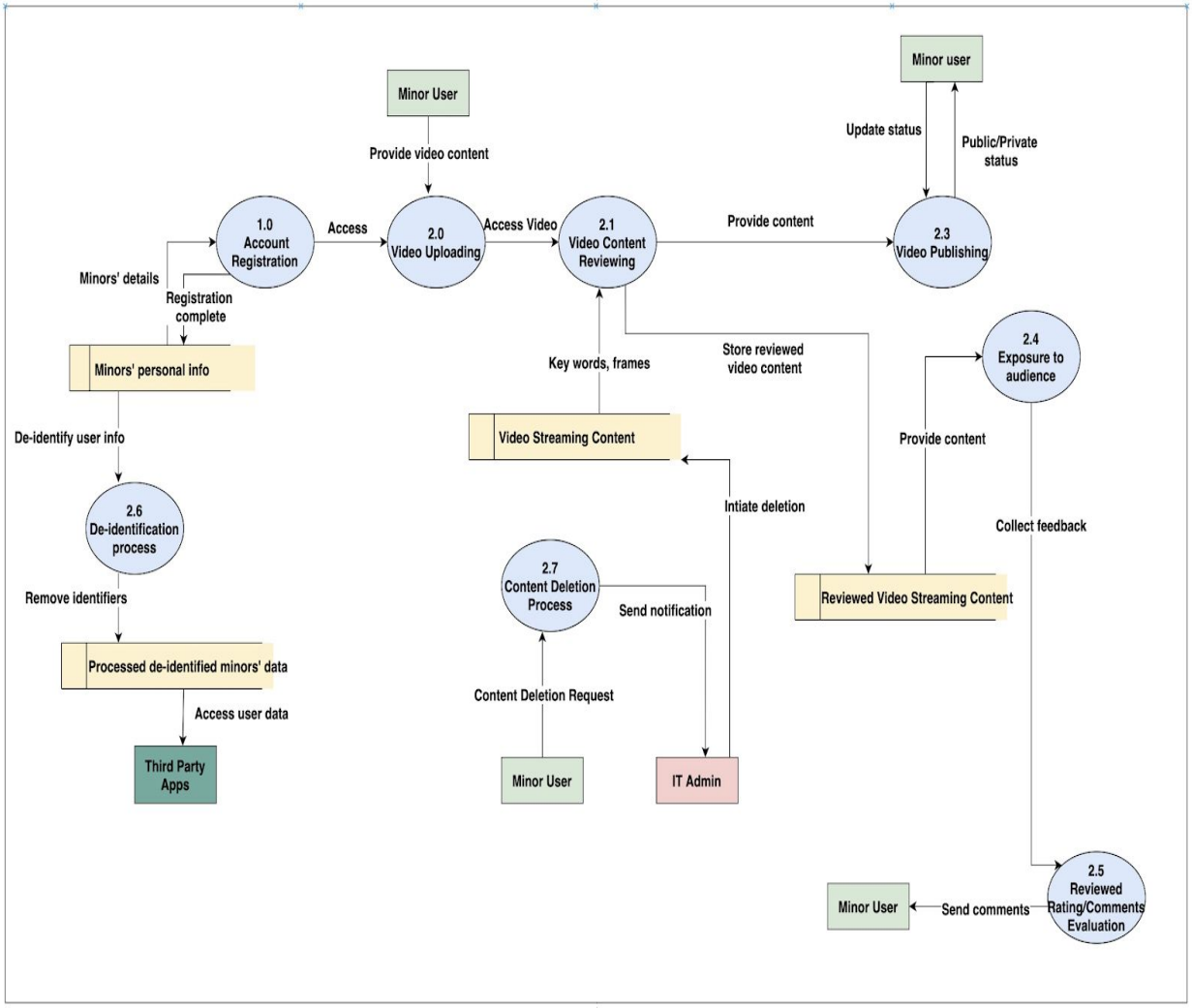

Figure 3 Level 1: Current State Data flow Diagram of Tiktok

Figure 4 is showing the Level 1 Future State Data Flow Diagram for Tik Tok scoped for GDPR according to our findings and solutions. The highlighted arrows in red demonstrates our suggestion in the form of a data flow diagram.

As discussed in our article further, we will describe how and why these changes can be beneficial. We have addressed various concerns and come up with solutions and implementing them through the data flow changes as indicated below.

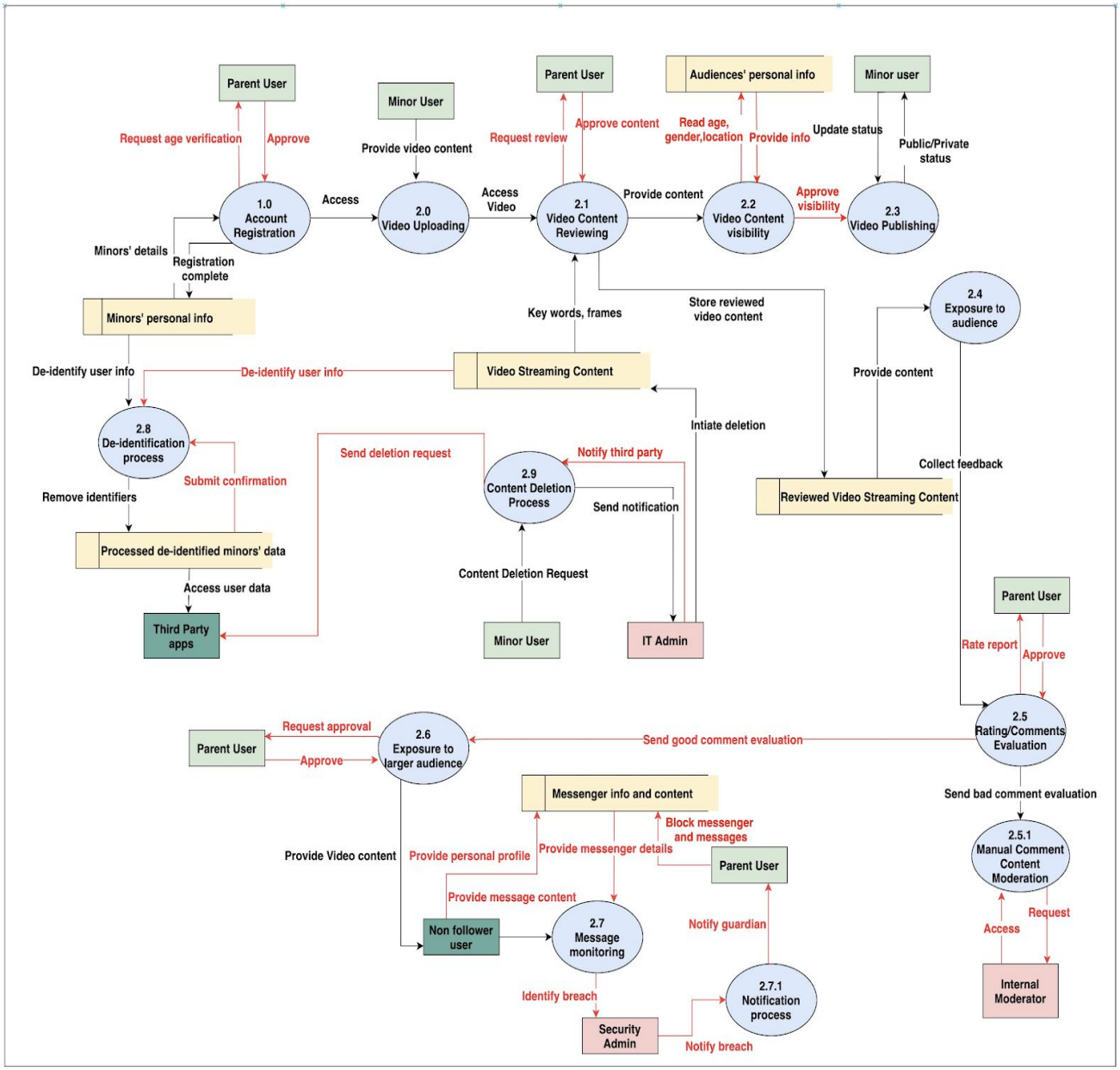

Figure 4 Level 1: Future State Data Flow Diagram for Tiktok (Scoped for GDPR)

DAMA Analysis

Data overview

Not only European Commission, but all other regulatory organizations recognize personal data as a highly valuable economic asset. Its value sometimes can be referred to as the "oil of the internet and the new currency of the digital world [14]." Since data resources could be used either in good ways or bad ways. Since TikTok is designed for engagement, its algorithms steer

people to video content via a "For You" page. So, it is easy for potential criminals to keep an eye on the minor targets by liking videos, sending messages. By learning from the data, the algorithm keeps showing similar video contents for potential criminals. TikTok collects a vast amount of data on minor users including:

- apps activity data such as which videos are watched and commented on
- location data
- phone model and operating system used
- the keystroke rhythms people exhibit when they type [13]

There are two categories of collection: automatic collection and collection under permission. The app automatically collects and stores browsing and search history within the app. Additional data can be collected based on user permission such as user age, user-generated content such as photos and videos; and the videos “liked,” shared, watched all the way through, and re-watched [13]. We suggested that TikTok should provide sufficient minor protection as soon as possible. We will talk about TikTok’s current practices regarding data storage, data security, data quality and management, as well as our analysis and solutions in these areas.

Data Storage

There has always been news flooding about how and where Tik Tok stores US users’ data. Initially TikTok has always refused to acknowledge where its data is stored, but recently after several global questioning and allegations about Chinese government getting hold of users’ data, Titkok has confirmed it is a false accusation and the data is stored in servers in the US, with backups in Singapore. Although Titkok has refused to make such allegations, there are private and government agencies who are concerned about the misuse of users’ data if it goes under wrong ownership and they are carrying on their own fact check to verify the situation.
In one of the recent news events about the data storage of US users, President Donald Trump has agreed to let TikTok operative in the US on one condition. The condition is to provide the ownership of data storage to US based organizations.

Oracle will be the next cloud provider for TikTok’s data [9]. It will quickly deploy, scale, and operate TikTok systems in the Oracle Cloud through delivering a highly secure environment and ensure data privacy to TikTok’s users globally. Oracle’s cloud technology provides private and secure for TikTok’s users with its continuous code reviews, monitoring, and auditing implementations. We will see if Oracle’s cloud works better for TikTok.

Data Security

Below is our analysis on current and suggested data security of TikTok -

(i) Minor's Age Verification: Currently, TikTok gets the age verification of minors through their email address. After studying this process, we found that this method is not very accurate and can easily be bypassed. We have proposed the idea of getting minor's age verified through his/her legal guardian, by sending them a notification and asking for approval.

(ii) Third party app access: Currently, users' data including minors are all shared with the third party apps associated with TikTok. Having minors' data floating all around third party apps can be dangerous. While we also understand from TikTok's business point of view why this data flow is important for their business. We have proposed an idea of de-identification of minors' data before it is being shared to third party apps. TikTok can introduce this process and filter out all the sensitive information and then it can be shared to third parties. This could be a potential and balancing solution for the organization.

(iii) Right to erasure: TikTok is well familiar with the 'right to erasure' from the GDPR regulations. TikTok currently accepts the content deletion requests from all its users and processes the request by deleting the content from their platform. While this sounds to be perfect, we found a loophole here. What happens if the content has already been shared on other platforms via third party. TikTok does not take responsibility for the deletion from there. This is understandable considering the vastness of the internet, but minors' data is more important than this and we have an idea that might do some damage control. We propose that TikTok after getting the request from the user and deleting content from their platform, can at least send a notification to their third party clients about the users' request. This step by TikTok will show their responsibility and concern towards their users and can bring back more user trust.

(iv) Content visibility security: Recently TikTok has introduced a process to review the video content uploaded by minors' before publishing it on the platform and making it visible to the audience. This process has been successful in filtering out malicious and inappropriate content. But what happens when a minor chooses this visibility to be 'public', his/her video can be seen by any group or range of audience. This poses a threat of Stranger Danger to the minors. To combat this situation, we are proposing a proactive step by TikTok to add a filter to the audience by their age, gender,location ,before any minors' video is visible to them. This way we can protect the minors' data from being passed on to unknown territory and protect them from Stranger Danger.

Data Quality and Data Management

There are several mechanisms we added to improve TikTok's current mechanism-

(i) Parent digital literacy: The series of parent approval requests we have added will also improve the digital literacy of parents and enforce verifiable age and consent provisions. As a result, these actions will improve the data quality and data management in return. Parents will only use the right of consent properly to the processing of their children's data if they are digitally literate and have the requisite knowledge to understand terms of privacy service. To achieve parent digital literacy, it will require close cooperation and communication between data protection regulator, TikTok data security professions, and parents.

(ii) Video content data: TikTok currently provides machine reviewing and human reviewing about the video content. We propose to improve this function by having parents approve the content. The research indicates that teens are easily to be induced or unintentionally post inappropriate videos. This function will help TikTok to improve management of the video data.

(iii) Video comment data: Parent has the control of whether to allow the video to expose to the larger audience according to the comment. TikTok currently has codes to detect comments with bad words or comments that contain malcontents. We propose to add an additional function which could send the comment report to parents. Parents would have the choice to allow or not allow certain comments being posted under the video. We also propose a functional process to collect all good comments in the database, and send the summary report to parents, and provide them an option to allow the video to be exposed to the larger audience or not.

(iv) Message data: Currently TikTok is introducing parental controls to minor users worldwide. The features will allow parents to disable on all Direct Messages for their teen users in all markets. We improve this function with reviewing and screening out messages containing suspicious words or messages from suspicious senders. This function is able to send notification to parents while senders from above try to send messages to the minor, providing parents the right to block these messages. Compared to the function TikTok already has, instead of the complete ban from all Direct Messages, our improved mechanism provides minor users with more freedom and liberty to use social media.

(v) General data maintenance: We also add mechanisms that ensure that the Personal Data processed is kept accurately and up to date. TikTok is able to match and update parent and child data to the "reasonable extent". The Personal Data of minors must be reviewed and updated no less often than on a quarterly basis. We suggest adding the GDPR compliance system of record to the security team to scope for GDPR its data processing activities.

CRUD Matrix

Entity Process	Minors Personal Info	Video Streaming Content	Audience Personal info	Reviewed Video Streaming Content	Messenger info and Content	Processed de-identified minors' data
Account Registration	**RU**					
Video Content Review Service		**R**		**CRUD**		
Video Content Visibility Service			**R**			
Audience Exposure Service				**RU**		
Message Monitoring					**RUD**	
De-identification Process	**RUD**	**RUD**				**CRUD**

Conclusion & Recommendation

Tik Tok has been in the process of changing its data management policies and improving it in order to comply with GDPR and other regulations. In 2019, Titkok had to pay a huge fine of $5.7 million to settle Federal Trade Commission allegations that the company illegally collected personal information from children [6]. While working on this project, we closely studied the data management framework of Titkok and the most current changes they are making, especially to safeguard minor users' data and their rights. We found that TikTok has introduced parental control features on certain levels to comply with GDPR Article 8 (especially for minor users).

TikTok has already been working on the changes. Under this project, we have come up with different suggested changes in the data architecture and data flow of the organisation to make it even more secure, reliable and strongly comply with GDPR. We have found some vulnerable

areas in terms of data privacy , data security ,data quality and data storage of users (mainly minor users). We have discussed all our findings and suggested solutions above in our analysis and DFDs. Some of them are - getting the minor's age verified from the authorized parent, extended use of de-identification process, responsibly handling content deletion requests etc.

TikTok might not need to add this step right away, but if they do, Titkok will become a more secure platform from minor users, it can bring back trust of the parent. Currently there are many parents who are skeptical about their minor child using TikTok, building a relationship based on trust can further nurture their business and help TikTok generate greater revenue. Our changes strongly and proactively complies with GDPR keeping in mind about the future changes. Adapting these changes, TikTok can assuage fears of ugly penalties from the government of different countries. The government agencies will also have a sense of reassurance and it will be easier for TikTok to smoothly run their operation all over the globe without getting governmental and political hits.

The findings and suggestions in this project clearly indicates that TikTok can greatly benefit from increased revenue . By having a robust data architecture complying to GDPR, TikTok will also automatically comply with most of the other region wise regulations e.g CCPA (California Consumer Privacy Act), Brazil's *Lei Geral de Proteção de Dados* (LGPD), United States federal law COPPA (Children Online Privacy Protection Act, 1998) . TikTok's data management cost will be reduced. TikTok will need to spend less time and resources in managing their data and they can use those resources to expand their user base. Having a large user base will give a competitive advantage to the organization.

We live in a very dynamic world and this age is data-age. Every day data is changing, demand is changing, new technologies are coming up, GDPR regulations are not going to be constant either. They have to change as the technology changes, proactive steps to comply with GDPR is never going to harm any organisation.The suggested solutions sounds like killing many birds with one stone.

References

1. Urquiola, Karla Badillo, and Pamela J. Wisniewski. "'Stranger Danger!' Social Media App Features Co-Designed with Children to Keep Them Safe Online." *Acm.Org*, 12 June 2019, dl.acm.org/doi/pdf/10.1145/3311927.3323133.

2. "TikTok Privacy Policy." *TikTok.Com*, TikTok, www.TikTok.com/legal/privacy-policy?lang=en. Accessed 2020.

3. "TikTok Privacy Policy for Younger Users." *TikTok.Com,* TikTok www.TikTok.com/legal/privacy-policy-for-younger-users?lang=en. Accessed 2020.

4. "Conditions Applicable to Child's Consent in Relation to Information Society Services." Intersoft Consulting, Intersoft Consulting, gdpr-info.eu/art-8-gdpr. Accessed 2020.

5. Kosta, Eleni, and Milda Macenaite. "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?" *Taylor & Francis Online*, 1 May 2017, www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096.

6. "Video Social Networking App Musical.Ly Agrees to Settle FTC Allegations That It Violated Children's Privacy Law." *Federal Trade Commission*, Federal Trade Commission, www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc. Accessed 27 Feb. 2019.

7. Kang, James Jin, and Paul Haskell. "What Kind of User Data Does TikTok Collect and Where Is It Stored?" *Scroll.In*, 20 July 2020, scroll.in/article/966871/what-kind-of-user-data-does-TikTok-collect-and-where-is-it-stored.

8. Intersoft consulting. "General Data Protection Regulation." Gdpr-Info.Eu, gdpr-info.eu/chapter-3.

9. Oracle. "Oracle Chosen As TikTok's Secure Cloud Provider." Cision PR Newswire, 20 Sept. 2020, www.prnewswire.com/il/news-releases/oracle-chosen-as-tiktok-s-secure-cloud-provider-818881202.html.

10. Chapple, Craig. "TikTok Crosses 2 Billion Downloads After Best Quarter For Any App Ever." *Sensortower*, 29 Apr. 2020, sensortower.com/blog/tiktok-downloads-2-billion.

11. European Commission. "Data Protection in the EU." *Europa.Eu*, 2018, ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

12. Rosenbloom, Michael, and Angela J. Campbell. “Before the Federal Trade Commission Washington, DC 20580.” *Commercial free childhood.Org*, 14 May 2020, commercialfreechildhood.org/wp-content/uploads/2020/05/tik_tok_complaint.pdf.

13. Scroxton, Alex. “TikTok’s GDPR Compliance Probed amid Accusations of Data Misuse.” *Computerweekly.Com*, 21 Aug. 2020, www.computerweekly.com/news/252487939/TikToks-GDPR-compliance-probed-amid-accusations-of-data-misuse.

14. Miettinen, Samuli, and Tobias Bräutigam. *Data Protection, Privacy and European Regulation in the Digital Age*. Unigrafia Helsinki, Unigrafia, 2016, books.google.com/books/about/Data_Protection_Privacy_and_European_Reg.html?id=AhkvygEACAAJ.