Ethics and Data Protection Framework

Working Document for Cilter
This document will be periodically updated and reviewed.
Last modified: 2019-07-08

Author(s): Harshvardhan J. Pandit (ADAPT Centre, Trinity College Dublin)

Background: Cilter is a child-protection software available via smartphones that analyzes data and filters it for offensive content. It also alerts parents if there is a perceived threat or risk to the child.

Motivation: This framework project was commissioned by Cilter Technologies Ltd to advise upon the best practises that should be adopted to safeguard children's data, remain compliant with applicable laws and regulations while delivering on 'privacy by design' that is ethically driven by integrating these recommendations at an early stage.

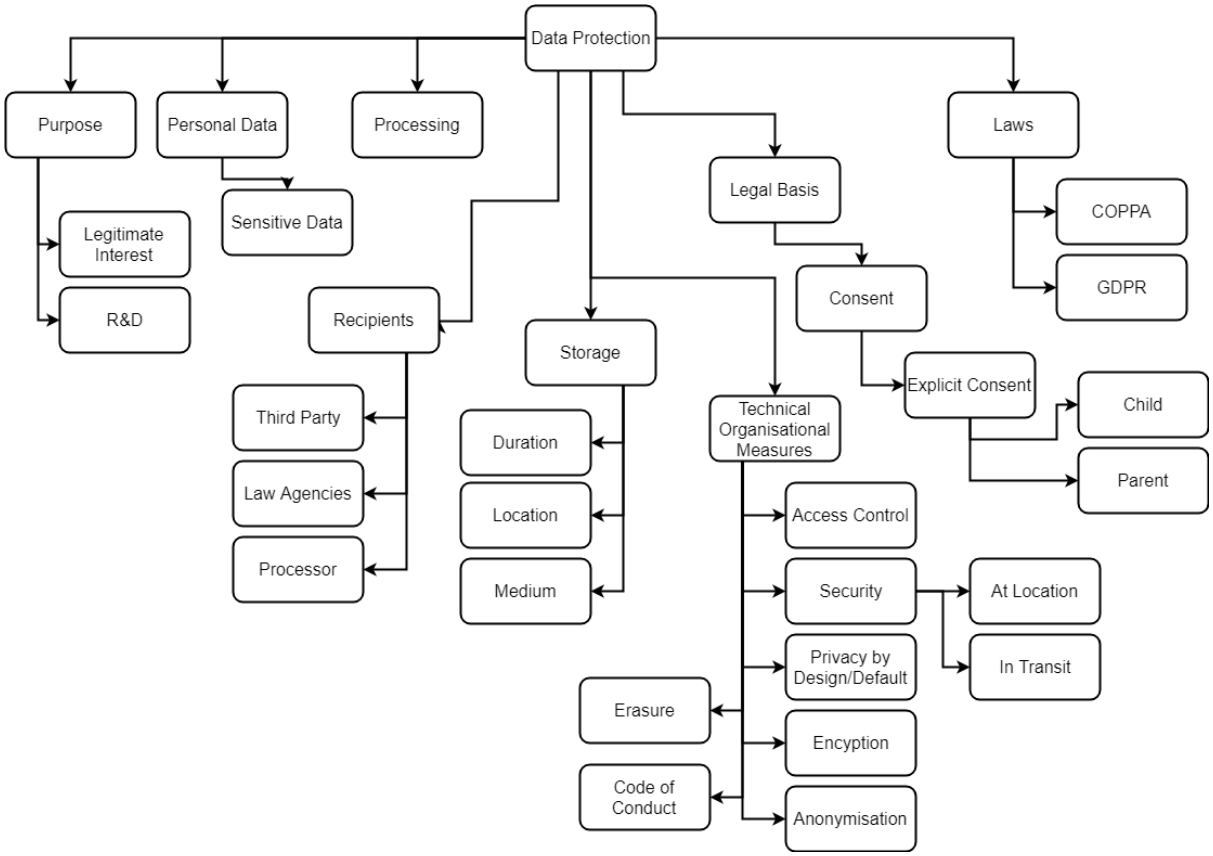
Applicable Privacy Laws

Question: What are the laws applicable for the processing of children's personal data?

Depending upon the jurisdiction an organisation operates in, it will be subject to one or more laws regarding data protection and privacy. Chief amongst these is the European General Data Protection Regulation (GDPR), which applies to all scenarios where the individual is a citizen of the EU or where the organisation operates in a member state. Its corresponding laws in the USA are the Children's Online Privacy Protection Act (COPPA). In terms of data protection (in general), the GDPR is currently the 'gold standard' in terms of transparency and legal requirements for data protection due to its comparatively restrictive set of compliance requirements. By being GDPR-compliant, the organisation thus also covers and sometimes exceeds the requirements specified by other privacy laws such as the Children's Online Privacy Protection Act (COPPA).

Recommendation: Choose GDPR as the global default for applicable privacy law in addition to other relevant local privacy laws applicable to the jurisdiction. Since Cilter would be processing personal data of children, COPPA compliance is also a necessity. Therefore, choosing measures and requirements that are more stringent (i.e. strict) from both GDPR and COPPA will provide a more secure and robust data protection framework. This will also allow Cilter to be both GDPR and COPPA compliant in its operations.

Information about Data Processing Operations



Personal Data

Question: What personal data is Cilter collecting?

As Cilter will be collecting and using ALL data within the context of a smartphone, it is important to specify what this data will or could contain. Specifics will need to be provided (as much as possible) regarding specific categories of data - and its metadata. For example, the abstract category of “messages” can be specified to indicate collection and usage of text messages (SMS) or messaging apps (e.g. Snapchat, Facebook, WhatsApp). Greater transparency requirements would dictate the specification of the exact nature of messages - such as whether the text is collected, if it is collected from all notifications on the phone, if it may include images or videos being sent. Additionally, if metadata is being used - such as who is sending the message or at what time - then this should be specified as well.

Depending on the jurisdiction and the privacy law, different terms are used to indicate categories of data which are sensitive or special in nature and carry explicit obligations regarding their processing. For example, GDPR mentions special categories of personal data (A9), while COPPA mentions Personally Identifiable Information (PII).

In addition, other forms of ‘personal data’ may also be collected and used by Cilter which may not usually be expressed or indicated as common practice, for example - device identifiers, cookies or similar technologies. This information is legally classified as personal data under the GDPR, and therefore requires notifying individuals about their processing.

Greater transparency can be achieved by explicitly stating the specific instances of what such categories of data contain - similar to the previous example regarding data associated with messages. This will enable balancing of privacy risks often involved in analysing and profiling individuals based on the use of identifiers and trackers in devices.

Recommendation: Identify and categorise personal data Cilter is or may collect. Specify whether the category or instance of personal data is explicitly mentioned within laws such as GDPR (special or sensitive) and COPPA (PII). Additionally, mention the use or non-use of any other personal data categories relevant to the individual which may be collected and used either explicitly or implicitly through the use of (third-party) technologies.

Purpose

Question: Why is Cilter collecting personal data?

While the main or primary purpose of Cilter can be stated as “filtering out harmful or offensive content”, there will be other purposes for which Cilter will or may require to process personal data. Examples are Research & Development (R&D), compliance with legal obligations, and marketing. Such purposes need to be clearly defined and separated from the primary purpose in order to determine their legal basis and compliance requirements.

Recommendation: Distinguish between the primary purpose of Cilter and identify other purposes for which Cilter is or will require to process personal data.

Processing

Question: What is Cilter doing with personal data?

Most privacy policies state the processing of personal data using common abstract terms such as - collect, use, analyze, store, and share. While these are sufficient to obtain legal compliance, greater transparency can be achieved by expanding upon the processing operations to explicitly state what Cilter does or intends to do with the personal data. As an example, consider - ‘analyze in the cloud’ and ‘analyze on your device’ - which makes it explicit where the data is being analyzed. Depending on what technologies are being used, there can be information about a particular algorithm or method attached to processing, such as - “analyze using automated machine learning” or “reviewed by staff member” to explicitly state the actors involved.

Recommendation: Clearly specify what processing operations are carried out over personal data. Consider attaching contextual information regarding how the processing is taking place, and the actors involved (whether automated or human) in the interest of transparency.

Recipients

Question: Who is Cilter sharing personal data with?

Where personal data is shared with any entity other than Cilter, the entity constitutes as a recipient of personal data. Such entities must be identified along with the role they play in the sharing of personal data. For example, Cilter may store their data using cloud services such

as Amazon - which will be a Data Processor acting under Cilter in this case. Where Cilter is required to share personal data with legal bodies or organisations by law, such entities should also be mentioned as recipients (where permitted by law). One of the chief concerns regarding privacy is the sharing of personal data with ‘third parties’ - entities who receive personal data from Cilter but are not Processors. GDPR requires such third parties to be named along with the provision of some information based on their location and jurisdiction. Where personal data is not shared with any third party, it is imperative to state this explicitly in the policy. Additionally, laws such as GDPR allow only categories of recipients to be provided, such as for Processors. In view of transparency, each provider may be explicitly mentioned along with their policies and contractual obligations with Cilter.

Recommendation: Identify recipients of personal data and their role - such as Data Processor, legal body or organisation, third party. Specify explicit information about the recipient such as name and jurisdiction rather than their categories.

Question: Why is Cilter sharing data with a recipient or third party?

When data is shared with any entity other than Cilter, the sharing must serve some determinate purpose, which is agreed upon by Cilter either through an agreement or through obligations dictated by legal bodies such as courts and laws. For transparency, the purpose and context governing the sharing of data should be made explicit. For processors, this would be the purpose and processing operations, whereas for cases where information is required to be provided by law - the specific law must be stated as a legal obligation.

Recommendation: For each entity the data is shared with, provide information about the role played by the entity, as well as the context of sharing - i.e. whether through an agreement or legal obligation.

Question: What data is shared with a recipient or third party? And what will happen to it?

When data is shared with any entity other than Cilter, the nature of relationship between the entity and Cilter must be transparent. For example, if the entity is a data processor, then it is obligated to act only on the explicit instructions of the controller i.e. Cilter. In such cases, Cilter has the means to explicitly state the purpose, processing categories, and personal data categories involved in its agreement with the processor. In contrast, when such an entity is a legal body, it may not be possible for Cilter to dictate or even identify the purposes or processing operations carried out by the entity. This also should be explicitly stated in the interest of transparency.

Recommendation: Where data is shared with each entity, specify the categories of personal information shared along with known purposes and processing operations. Where this information is not known, the reason and context should be made explicit.

Storage

Question: Until when does Cilter store personal data?

Where Cilter stores the collected data, the duration of storage should be based on either a clear condition or event (e.g. closure of account) or temporal (2 years from last collection). Often, such information is abstracted or stated in a way which makes it difficult to determine the exact extent of storage duration for personal data. Therefore, a common policy or condition can be adopted as default for all or a group of personal data (or associated with a purpose), with deviation being explicitly mentioned in order to convey the information in a simpler manner. For example, all data can be stated to be stored until closure of account, except for name and address which are retained for an additional 2 years for legal reasons.

The location where personal data is stored also affects how the privacy laws apply. For example, under GDPR, storing information within the EU (or an equivalent jurisdiction that has appropriate safeguards) is a requirement. Therefore, the location of personal data is required to be explicitly identified and stated. Where possible, personal data could be stored locally to ensure compliance requirements of local regulations are met. For example, personal data of individuals in EU is stored on cloud servers physically located in the EU, while those for USA are stored correspondingly within cloud serves in USA.

Recommendation: Have clear storage durations in the form of event/condition or temporal duration/expiry-date for all purposes and personal data. Where possible, adopt a suitable default storage duration for personal data to simplify the process of determining and conveying information.

Question: Where and how does Cilter store personal data?

Where Cilter stores data, such as the device or the cloud, should be made explicit. In cases where data is stored in both mediums, it should be explicitly stated as such. The purpose of storage should also reflect its necessity of being stored on a particular medium, such as whether the storage is meant as a backup or archive. Finally, the form the information is stored in should also be specified where possible and necessary. For example, if the information is stored in using device-specific APIs or features, such as for smartphones. This provides important information regarding the safety and security of the storage, as in some cases these would be dependant on the APIs provided by a service or device.

Recommendation: For each instance of storage, identify the mediums of storage, their purpose or context, along with how the information is actually being stored - such as through APIs or libraries in order to determine their safety and security.

Question: What are the legal jurisdictions where data is stored?

The specific legal jurisdictions, where applicable, need to be identified for the storage locations of data, as this affects the individual in terms of laws applicable. Where storage is duplicated across jurisdictions, this may have effects on the individual in terms of access to information by legal agencies and legislations. This is applicable for cases such as cloud backups - which call for data to be spread in geographic locations for purposes of security, access, and performance. Cases where the data storage location is in a separate jurisdiction than the individual should also be identified or made implicit through information provided.

Recommendation: Identify the legal jurisdiction of data storage locations, and their relation to the individual. Where the jurisdiction is different from that of the individual, this should be informed by explicit (specifically mention difference in jurisdiction) or implicit (only mention the jurisdiction of data storage) means.

Legal Basis

Question: What is the legal basis or justification used by Cilter to process personal data?

For each purpose and processing undertaken, the appropriate legal basis or bases should be identified, evaluated, and documented for each applicable legislations. Where different legal bases are required based on jurisdictions, Cilter has the option to choose the more ‘ethical’ or ‘stricter’ legal basis - such as consent where legitimate interest would suffice. Such decisions should be made explicit to the individuals, and should be part of the agreement or contract between them and Cilter.

Recommendation: Cilter should specify the associated legal basis or bases for each purpose of processing in order to specify the necessity as well as requirements associated with it. Where Cilter chooses to use a different legal basis or action other than what is strictly required by law, it should provide information on its decision and consequences in a transparent manner.

Question: What are the legitimate interests used by Cilter to process data?

Where legitimate interest is used as the legal basis, Cilter should provide a clear explanation of what the interest is, and how it is justified to be of necessity to its operations. This explanation may consist of the justification for why the purpose is necessary for operations and why Cilter believes it does not infringe any rights or bring upon harms or risks to the individual.

Recommendation: For purposes where legitimate interest is used as the legal basis, provide a clear explanation of what the interest is, with a possible statement regarding how it is balanced against the rights of an individual along.

Question: Where is consent used as the legal basis?

The use of consent as a legal basis implies the individual has control over the decision of whether they permit their personal data to be processed. Consent by itself does not constitute a legal basis, it is only when it is used to justify a processing purpose that it becomes the justification for that processing. Consent can also be used to provide control over operations other than it use as a legal basis for processing - such as for operations not involving personal data. However, when used as a legal basis to justify processing of personal data, acquiring consent has several obligations associated with it depending on the jurisdiction and law applicable. Therefore, it is vital to identify and specify where the consent being used is a legal basis, and places where its provision is a choice made by Cilter in order to provide more control to the individual.

Recommendation: Specify where consent is used as the legal basis, the laws applicable to it, and for what purposes of processing it is applicable. Similarly, where consent is not used as a legal basis, but provided as an additional form of control to the individual, this should be specified as well.

Question: What legal obligations or requirements are applicable as legal basis?

In cases where Cilter is required to perform activities, that may or may not involve personal data, based on legal requirements or obligations, such laws should be identified along with their jurisdictions. This information should be clearly provided to individuals affected where possible, along with links to more information on the topic.

Recommendation: Where Cilter is required to undertake any activity by law, including processing of personal data, it should provide this information including the specific law and obligations.

Question: What actions does Cilter perform in the protection of vital interests of individuals as a legal basis?

Where certain actions or activities are undertaken in order to protect an individual's vital interests, the specific vital interest should be mentioned, if possible. The actions or activities should also be explained in terms of what they constitute, how they are undertaken, whether they are automated or explicitly decided by a human. Information on how the information is communicated, including to whom (recipient), should also be provided. Where possible, the source of this information in terms of recipient should also be provided. Cilter should also indicate whether the individual has any control over the actions performed, such as whether it can override or cancel a particular action.

Recommendation: Activities undertaken to protect the vital interests of individuals, including alerting authorities or parents, should be explicitly made clear along with information of what each activity constitutes, how it is detected/decided, and how it is communicated.

Consent

Question: Where does Cilter require consent?

Consent indicates an access mechanism to the use of a service or feature for a particular purpose to the individual, where giving consent enables the processing of personal data for that purpose. Consent can also be used to provide an additional layer of control to the individual where the choice to continue is explicitly indicated by the individual, and which implicitly indicates the possibility of withdrawal or revoking of consent in the future. Based on the use of consent as a legal basis, obligations and requirements come into picture - such as those for GDPR - which shape the experience of obtaining consent. Therefore, a clear indication of areas or features where consent is used is necessary, along with information on where the consent is a legal necessity, and where it is provided as an additional control for the benefit of the user. Simultaneously, the degree of control afforded by consent should also be made explicit to the individual - for example, by indicating that processing of

personal data is based solely on the provision of consent, and that without it, the processing will not take place.

Recommendation: Where consent is provided as a legal basis or otherwise, clear information should be provided on its use to enable access to services or features, and the implications for both - granting or refusing - consent should also be communicated.

Question: How does Cilter acquire consent?
Question: Where consent is provided by a delegate, such as a parent, how is the relationship verified?

In cases where Cilter acquires consent and the consent itself is a legal basis or justification, the mechanism used to obtain consent should be shaped by the obligations and requirements of the law. For example, GDPR specifies that consent for special categories of personal data should be informed as well as explicit - which should be reflected in the medium and context of the mechanism used to obtain consent. Therefore, an indication and evaluation of how and where the consent is acquired or obtained should be documented, and where possible - indicated to the individual. For example, consent can be acquired when first signing up to the service on Cilter's website - in which case, the consent mechanism would be provided through the website itself.

At the same time, consent is not bound by the medium itself - for example, the smartphone used in the provision of services is also bound by the same consent, and therefore is also a valid medium for interaction of consent. Therefore, an exploration of where Cilter needs consent, and how that consent should be collected should be undertaken along with the question of how consent can be interacted with across devices. This also brings up the question of identity verification or association of identity of the account or activity with the individual. For example, if consent can be given or revoked by anyone with access to the individual's smartphone, this implies access to smartphone is an indication of the individual's identity. Therefore, these situations should be made clear along with the expected role played by the individuals in the context of consent.

Recommendation: The mechanisms used for obtaining and interacting consent should be clearly indicated along with information on the roles played by different entities in the process. This can involve the role of delegates (such as parents), or even processors acting on behalf of Cilter to provide services such as identity verification.

Question: What information is provided when acquiring consent?

The information provided when acquiring consent is dictated by the legal requirements in cases where it is a legal basis for processing. These requirements indicate a spectrum of information provision such as informed and explicit where one end is only concerned with the acquisition of consent in the form of an implicit action by the user, and the other end is concerned with obtaining the strictest possible measure of consent based on the individual's understanding of what they consent to. The latter measure can be interpreted as the basis for explicit consent under the GDPR, and is the strictest measure currently enforced by legislation in terms of data processing. Similar measures exist in the medical and health domain, where the consent of patient is required to follow stringent requirements based on

the provision of information and the action indicating giving of consent. In the case of Cilter, the information provided for any consent, whether used as a legal basis or not, should follow this strict interpretation of explicit consent, where as much information as can be reasonable to be understood by the individual should be provided.

Under GDPR, the information to be provided includes information regarding the purpose of processing, the categories of processing operations, categories of personal data including explicit mention of special categories of personal data, recipients, and data transfers to locations outside the EU (and aligned jurisdictions). This information can also include specific conditions or durations associated with storage, the presence or use of technological measures such as encryption, and an indication of any risk based on the type of processing used. This should be used as the default template for all information being provided to the individual in order to ensure complete transparency and enabling trust regarding the operations performed by Cilter.

In the case of children, this information should be simplified without compromising on the overall intended indication of its purpose. For example, assuming that children may not be capable of understanding technical information regarding the storage of data, simplified forms may include the use of abstractions and analogies, such as - “storing information over the internet similar to how Facebook or Instagram stores it” depending on the intended age and comprehension capabilities of the individual. At the same time, information provided to parents should focus on providing as much transparency as possible and should indicate links to further information where it is not possible to include the entire information in the given context.

Recommendation: Document the information provided when obtaining consent along the requirements for informed and explicit consent, with the information being made suitable for the intended individual’s age group.

Question: What measures are in place to handle withdrawing or revocation of consent?
Question: What happens after consent is withdrawn or revoked in terms of personal data processing or service provision?

Consent can be interpreted as a one-time action enabling the processing of personal data without possibility of future revocation. However, such an interpretation is not valid under the legal definition of consent under laws such as the GDPR, where the withdrawal of consent is a right provided to the individual. In cases where consent is used as the legal basis, the withdrawal forms an obligation that needs to be addressed. Therefore, in cases where consent is not a legal basis and is asked without a measure for its withdrawal should instead use the legal term of ‘agreement’ to indicate acceptance instead of consent.

For cases where consent is used, there should be information provided regarding how the given consent can be changed or withdrawn, along with an easily accessible link or mechanism where possible. For example, when asking for consent online, information can be provided regarding where consent can be withdrawn - such as through a link at the bottom of the page. Information should also be communicated regarding the consequences of withdrawal of consent, such as whether certain services or features depending on the consent would stop working.

How such changes or withdrawals of consent would be handled internally should also be documented. Particularly with respect to the technical measures which ensure that processing based on consent incorporates the change in order to stop further use of personal data associated with the consent.

Recommendation: Document measures for handling the withdrawal or change to consent along with the technical approaches for ensuring such changes are reflected in the processing and services. Also document information regarding how the individual can access mechanisms for change and withdrawal of consent along with its impact on individual's access to services and features.

Documenting Information for Compliance and Transparency

Question: How should information be documented with a view towards legal compliance and transparency?

Legal basis is the justification which Cilter will use to process the personal data it obtains. Guidance is available across jurisdictions for choosing the appropriate legal basis based on the specific privacy laws applicable in the jurisdiction. We will focus on GDPR as it provides a greater requirement for transparency regarding legal basis. Under GDPR, each data processing must be carried out for a particular *Purpose*, which can consist of one or more *Processing* operations on *Personal Data*. GDPR specifically mentions and provides additional requirements for certain processing operations such as *Recipients* and *Storage*. Each such purpose should have **one or more *Legal Basis* - such as legitimate interest, consent, or required by law.** In addition, the obligations regarding safety and security of personal data are expressed in the form of *Technical and Organisational Measures*, which denote what measures are taken regarding the processing of personal data.

Example: Cilter collects and uses (processing) name and email address (personal data) for contacting the individual (purpose), which is a legitimate interest (legal basis). Cilter stores the data for as long as the account is valid (data storage condition) as well as an additional period of 2 years (data storage period) for legal requirements (legal basis). It keeps this data encrypted and under access control (technical measures) in a secure database accessible only by employees under contractual agreement (organisational measures).

Recommendation: Cilter can achieve greater transparency in its practices by structuring its data processing operations in the form of a vocabulary, which can be represented as in the following table. This information should be reviewed periodically, especially after significant changes in the purposes or personal data utilised. Structuring the information in this manner will assist Cilter in meeting legal obligations such as those for GDPR, and also in the dissemination of this information e.g. through a privacy policy. A helpful resource for this is the Data Privacy Vocabulary (https://w3.org/ns/dpv) which provides some terms for expressing required information.

Purpose	Processing	Personal Data	Storage	Recipients	Technical and Organisational Measures	Legal Basis
Contact	Collect, Store, Use	Name, email	Until account is	None	Encrypted, access control, employee contracts	Legitimate Interest

			valid			
-	Collect, Store, Use	Name, email	2 years after leaving	None	Encrypted, access control, employee contracts	Required by law (link to law)

Technical and Organisational Measures

Question: How does Cilter ensure protection and security of personal data?

The protection and security of data is managed by technical and organisational measures, technical implies the use or involvement of technological solutions, and organisational implies measures involving human-resources. While not all technical and organisational measures need to be declared (publicly), their documentation is a legal requirement, while providing sufficient information to the individuals is obligatory depending on the level of information and services. For example, in general, it may be sufficient to merely inform that data is stored securely, whereas for special categories of personal data, it may be prudent to also mention the specific implementations to assure the secure storage. Cilter, as it intends to deal with sensitive content involving children, should target stringent measures backed by well-researched justifications with respect to the adoption of technical and organisational measures. Such measures are primarily focused on the areas of data storage, security, access, and human-resources in charge of oversight and management.

Recommendation: Identify risks and concerns regarding data storage, security, access, oversight, and human-resources, and determine appropriate technical and organisational measures to address these.

Cilter: There are a couple of key technical points that are used to ensure the protection of data from a safety and security point of view. The first is around physical storage and access. All data will be stored on virtual storage on a cloud based storage. There will be very limited access to this data, for example, certain devices from the Cilter network will have appropriate access for analysis of this data.

The next area is about the storage of the data itself, there will be application layer encryption applied to the data. This is helpful in preventing interpretation of the data on the basis that access is compromised. In this scenario, if data was accessed, directly, it is of no use, because it will have been encrypted from within the application layer.
Lastly, any data we need for Cilter to continue to evolve its offering to the marketplace will be supported by the anonymization of data. This means that we don't store direct personal attributable details about a user of the system.

Data Storage

Question: How/Where does Cilter store personal data?

For personal data that is stored, the context associated with storage affects a large portion of data security and safety in terms. This is because the storage medium and location affect how the data is protected, used, and accessed by both - Cilter and the individual. In terms of

location, different jurisdictions have differences in terms of laws and obligations that need to be followed. For example, under GDPR, the data must be stored in the same jurisdiction i.e. EU, whereas laws in certain under jurisdictions may obligate provision of access to legal authorities regardless of where the data is stored globally. Therefore, an indication of where the data is being stored in terms of location, and the laws applicable to it must be documented. This is applicable to both the individual user as well as any storage performed by Cilter or its contracted processors.

Categorisation of data based on where it is stored should be identified, such as which data resides on a device and what is based in the cloud. For cases where the data in the cloud is a backup or an archive of data on the device, it must be made clear with information on how the data is backed up or archived. Additionally, some cloud providers may automatically duplicate the data across jurisdictions for performance and safety reasons. The effect of this on the legality and processing of personal data needs to be evaluated based on the guarantees offered by the provider, although an awareness of whether and where this happens is a necessity to be undertaken by Cilter.

The specific technologies used to store the data also need to be identified and documented. For example, cloud providers have different categories of storage mechanisms such as for backups and archives, with differing guarantees of safety and resilience. These need to be identified along with their implication on the storage of data for Cilter. For smartphones, the storage is directed by the provided APIs which determine the technological basis for how data will be stored on the device. These also need to be documented along with an evaluation of how the data is stored in terms of security and access.

For information stored in a database, the choice of database and/or provider has an impact on the technological measures adopted. For cases where the database is hosted on a server or managed by a provider other than Cilter, the relationship between the server or database provider should directed by a controller-processor agreement. Furthermore, the location of the database or the server it is stored on should also be identified along the same guidelines as storage of data in terms of jurisdictions and its effect on the individual.

Recommendation: Identify what data is stored, and the means for storage in terms of technology used, location, provider agreement and guarantees, as well as use and effect of technologies such as APIs on the storage.

Cilter: All data will be stored on virtual storage residing in a secure cloud platform. Access to this data is restricted. There will be an access matrix defined which defines who and what devices have access to this data.

All data will reside in variety of standard SQL Relational databases. Backups will be encrypted, relevant data at rest will have application layer encryption applied, data in transit will have TLS1.2 at a minimum applied in addition to site to site VPN's for transmission. As part of selecting a cloud vendor, appropriate certifications will be sought.

Another key point about our data storage is there will be a real time transformation matrix applied to anonymize the data and separate the user from their user content activities.

Ultimately, we are applying privacy by design and that approach will also prevent any Cilter employees having the potential to compromise and privacy concerns.

Data Security

Question: How does Cilter ensure appropriate security of data?

Access Control

The first and foremost concern regarding the safety and security of data is the identification of who has access to the data. When dealing with potentially sensitive information, such as in the case of Cilter, it is vital to identify all possible means of risks and concerns regarding access to information, and to identify measures to mitigate them.

Where data is stored on the child's device, there needs to be sufficient information and guarantees regarding who has access to that information. While the way smartphones operating systems are structure provides some measure of guarantee regarding access to underlying data, Cilter should investigate whether this level of access is sufficient to meet its requirements. In this case, it should determine whether the device itself has a sufficient level of security associated with it - such as through the enforcement of a device lock code, and enabling encryption of data on the device. Furthermore, it should investigate the possibility of the information being accessed through technological means - such as the process of 'rooting' in the case of Android devices. Another avenue of device-dependant features is the cloud backup of data, which may include information deemed by Cilter to be sensitive.

For data stored in the cloud, Cilter should identify who has access to the information by investigating all possible means of access. Possible risks or concerns include - using the same APIs or services used by a device to access the data in the cloud to also access additional information, to use the provided security keys or access codes by the cloud provider, access obtained through the management console or service dashboard for cloud providers or services, attempts at phishing or using fraudulent identities to access information, and physically obtaining access to data. For data stored in databases, Cilter should additionally also investigate the possibility of leakage of credentials or its misuse, the creation of new users with access to information, and someone gaining access to the server or provider the database is stored within and misusing that access.

In general, there are also concerns that should be addressed regarding utilising known security shortcomings or malfunctions of technologies, as well as the possibility that a new security concern may be identified in the future. Where it is not possible to immediately mitigate a concern or remove possibilities of it being a risk, appropriate measures should be adopted to address those as they arise using both technical and organisational measures.

Data Encryption

Another form of security is the encryption of data, whether for storage or transmission. Encryption provides a measure of security in that the data cannot be readily read without the appropriate key required to decrypt the data. Based on the form of encryption used, the guarantees provided are strong enough to make it infeasible for the data to be decrypted

through brute force alone. Additionally, flaws in the cryptographic algorithms can be discovered which reduce the security associated with that particular encryption technique. Another area affects choice is the effect on chosen encryption algorithms on the performance. For example, it may not be feasible to use certain encryption techniques on a smartphone which has limited performance capabilities. In certain cases, the choice of encryption technique may also depend on existing implementations provided by the device or service - for example, through APIs on a smartphone or default disk encryption on cloud servers.

Encryption should be utilised at three key points of interaction regarding information. The first is the storage of sensitive data on the device or the cloud, where the encryption ensures the information is not accessible outside the parameters decided by Cilter. This also ensures the information is secured against unauthorised access, such as when the device data is copied to another location. The second is when data is being transferred or transmitted between the device and the Cilter servers. This form of encryption ensures that the information cannot be accessed or compromised, such as through man in the middle attacks. Internet protocols such as HTTPS and TLS should be utilised to take advantage of their inherent security in the use of encryption. Finally, the third concern is when Cilter communicates or facilitates communication such as for parents or the authorities. The transmission of this information in an encrypted manner is essential particularly when it is sensitive.

A valid concern when encryption is used is the control of keys that can decrypt the data. Even partial access to these keys can be sufficient to compromise the security of the information. Therefore, it is vital to also utilise security measures at an organisational level which ensure the sufficient security regarding storage and access to encryption keys. Similarly, different encryption keys could be used to prevent the compromising of one key from affecting all information. Keys can be used separately based on location, purpose, or any combination where it is possible to identify and isolate the compromised information.

Anonymisation

Because the information is particularly sensitive, strong forms of anonymisation techniques need to be identified and applied, with a particular emphasis on the re-identification aspect. This is because effective anonymisation is difficult in practice, or may not be possible in all cases. Therefore, it is better to consider information as pseudo-anonymised, with a certain level of difficulty associated with the de-anonymization process. Also, information that may generally be taken as anonymised may in actuality itself contain information that can identify an individual or a group of individuals. For example, a screenshot of a person’s name in a conversation - which can provide identifying information even when the metadata of the screenshot has been anonymised. Therefore, the exact processes of anonymisation and their impact on the information should be identified and documented. Additionally, the possibility of identifiable information in any form, such as for other individuals, should also be taken into account when categorised data as being completely anonymised.

Pseudo-anonymisation itself can also be used as a security feature, such that the information required to identify an individual or associate them with some additional information is kept separate from the other information. This prevents compromised

information from being associated with a particular individual or group of individuals. For example, separation of identity information and association with information within the database. The measures used to implement such pseudo-anonymised separation of information should be documented in order to determine their effectiveness.

Different information will have differing techniques for anonymisation. For example, in the case of text messages, only the individual's name may be anonymised but not their correspondents. This could be because of a variety of reasons, such as not being able to detect the names in a conversation or the use of nicknames. Furthermore, it may be possible that the conversation contains information about school or locality which can be used to potentially re-identify the individuals or narrow the search to a particular group of individuals in a geographic area. In this case, the conversation cannot be said to anonymised due to the presence of identifiable information, and would be pseudo-anonymised. In order to identify the risks and implications associated with this, the undertaking should evaluate whether such re-identification is possible at scale or affects a large and significant number of individuals. It should also assess whether the use of anonymisation makes such cases feasible or possible through its design.

Although information may be anonymised in one instance, such as on the Cilter servers, the same information could exist in a de-anonymised form in another location, such as a on another Cilter server or the individual's device. In this case, this information could be used to potentially re-identify the anonymised information, which could constitute a security risk.

Although, it is not required legally to require consent to store anonymised information, providing information about it is essential towards transparency. Additionally, anonymised data always has the potential risk of being de-anonymised by either using additional data or by exploiting a flaw in the anonymisation process. Therefore, records of the anonymisation process and its effectiveness should be documented and analysed periodically. Furthermore, the process of anonymisation does not necessarily lead to anonymised data, as it can potentially be de-anonymised. Therefore, this should be referred to by its correct technical term, which is pseudo-anonymised or pseudonymised data to indicate that it may be associated with individuals through some means. This can be done by using personally identifying information or identifiers which can link the data to an individual.

Privacy By Design

The privacy by design principles requires privacy to be a deciding factor when developing and operating services, such as through the choice of technologies used or interactions designed. The principle is a legal requirement under laws such as the GDPR, which requires information about it to be documented for compliance. Privacy by design incorporates technical and organisational measures regarding the protection of data and individual's rights, but also regarding the development of processes in which privacy is an important factor. For example, the interactions between a parent and the authority can be developed in a manner that ensures the privacy of the individual concerned while still achieving the objective of the communication.

Privacy By Default

The Privacy by default principle can be summed up to determine the ‘default’ choices or cases an individual may face, and to provide options which enforce privacy by default rather than requiring the individual to make an explicit choice regarding them. For example, opt-in rather than opt-out. This principle is a legal requirement under laws such as the GDPR, and therefore must be implemented in an appropriate fashion for all processing and interactions regarding personal data. The privacy by default principle is also applicable when choosing implementations such as storage locations or interactions, in which the more ‘private’ setting could be made the default. For example, use of HTTPS over HTTP when transmitting data. In this case, privacy also encompasses security, but which may not always be the case.

Data Deletion and Erasure

Because Cilter stores potentially sensitive information, the deletion and erasure of this information in a secure and safe manner is vital. Erasure of digital information can be tricky to determine because of the underlying manner in which information is stored, as well as the inability to control the actual data being stored, either on the device or in the cloud, because of the access being mediated by a middle layer provided by the device or service provider. Therefore, Cilter should identify options for deletion and erasure, and evaluate its risks.

Particular areas of concern are when the information is being stored via external or third party service providers, such as cloud servers. In this case, erasure should have guarantees regarding its effectiveness specified by the service provider. In the case of devices, such as smartphones, erasure can be difficult due to the structure of information storage and mechanisms. In all cases, storing information in an encrypted format can mitigate some of the risks associated with insufficient erasure, as the information recovered would still be encrypted, and therefore protected.

Organisational Practices

Apart from technological solutions, practices and measures also need to be addressed at an organisational level, such as through the enactment of policies or adoption of guidelines. By documenting such practices, an organisation is able to communicate their intention to the individuals and is socially liable to uphold them in all their practices. Some of the most commonly adopted practices include codes of conduct, design standards, staff training, certifications, and risk management procedures. By documenting such procedures, an organisation is able to demonstrate awareness and the existence of a plan to ensure privacy and rights of an individual, as well as procedures to mitigate risks and handle situations of concern. For example, by providing staff training regarding the sensitive nature of information and the need for additional protection of information, the risk of a staff member failing to incorporate sufficient measures regarding privacy is reduced. Similarly, codes of conduct provide a set of guidelines which dictate or shape development and operation of processes and services. Finally, certification or seals provided by a third party audit can act as mechanisms of trust to show the adherence of the organisation to a set of standards.

Operational Practices

Special Categories of Personal Data

With respect to the GDPR, there are several clauses explicitly relating to the personal data of children, and which would be applicable for any organisation acting or intending to act on the collection and processing of such data. That being said, a more proactive stance would be to consider and adopt the other clauses of the GDPR pertaining to sensitive information or special categories of personal data to create and provide a more robust and privacy-focused environment within the organisation.

Recommendation: Adopt all clauses of the GDPR pertaining to the processing of special categories of personal data in addition to the ones about children. This will lead to all personal data being considered sensitive or special category - which carries with it several obligations and requirements which will need to be satisfied. For example, under GDPR (A9), when using consent for special categories of personal data as the legal basis, the requirements need it to be 'explicit consent'. This could be provided at the time of signing in or creating an account with the service or at the time of first use. Furthermore, given the issue of age, the consent should be managed between both parent and children.

Data Protection Impact Assessment (DPIA)

Working with special categories of data carries with it the obligation to carry out a Data Protection Impact Assessment (DPIA), which should also be the case for processing involving children's personal data. The adoption of DPIA should be an ex-ante exercise rather a post-processing practice. This allows the organisation to be pragmatic about the impact of its technology on the rights and risks to children. Although not required by all jurisdictions, it would be pragmatic to undertake a DPIA at a global level for operations in order to ensure consistent transparency and trust.

A DPIA involves identifying the nature, context, scope of processing along with its necessity and legal compliance. It also involves the identification of risks and their assessment in terms of individuals affected, along with measures to mitigate those risks. The questions provided in this document, along with the various recommendations, should serve to provide guidance in the DPIA process. In order to ensure such risks are identified at an early stage, the DPIA should be conducted before services are put in to production/operation i.e. at the ex-ante stage. This allows a chance to mitigate those risks before any actual individual is potentially affected, as well as to ensure a certain degree to security for any activities that are put into operation. Similarly, in order to ensure that the processing being carried out also does not pose any risk, a DPIA should also be conducted for operations that have already been completed i.e. ex-post stage. This will allow identification of any new risks that may have arisen during the course of operation, and to mitigate them for affected individuals as well as other individuals in the future.

Recommendation: Integrate the DPIA process into the general workflow regarding development and deployment of any activity utilising children's personal data.
Recommendation: The DPIA should be utilised as both ex-ante and ex-post activity.

Rights of Individuals

The provision of rights is based on the law applicable and the jurisdiction it covers. By adopting all rights, except where they contradict each other, each individual is provided a larger set of rights regarding the protection of their data and privacy. To that end, the rights provided by the GDPR regarding the access and provision of information (covered by the data protection part of this document) enable transparency regarding usage of data and operations by Cilter. Therefore, such rights, where the individual is provided with more information and control should be adopted and enabled for all jurisdictions.

In GDPR, the right to be informed is concerned with the provision of this information before the data is collected and processing takes place, whereas the right to access is concerned with information about how the data was collected and processed.

The right to rectification allows individuals to have incorrect or incomplete data to be corrected. In this case, processes are required to assist the user in exercising this right, and also ensuring the updated information is correctly utilised in the future. The right to erasure (or the right to be forgotten) enables the individual to request their personal data to be permanently erased. In this case, when exercised by a child and consisting of sensitive information, the right may be confirmed with the parent based on the context of the request. Simultaneously, procedures on how such rights should be handled when the child reaches the age of adulthood (e.g. adults are defined as being 18 years of age in most jurisdictions where they obtain all of the legal rights for an adult) should also be in place, and communicated to the child as well as the parent in an appropriate context. In addition, Cilter should also adopt the practice of automatically deleting certain data after a reasonable duration, unless the data is still required.

Depending on the legal basis used, the right to restrict processing enables the individual to request that their personal data no longer be processed. Cilter should identify in which purposes and processing this right applies, and whether it can be readily exercised by the child or parent (or both).

The right to data portability enables the data subject to obtain a copy of their personal data (or have it transferred) in a safe and controlled manner and a machine-readable format. For Cilter’s operations, an identification of which information needs to be provided upon exercising the right should be undertaken, while also indicating which information may contain potentially sensitive information. In case of compromising or sensitive information being identified, Cilter can opt to provide the information only to the parent or the authority.

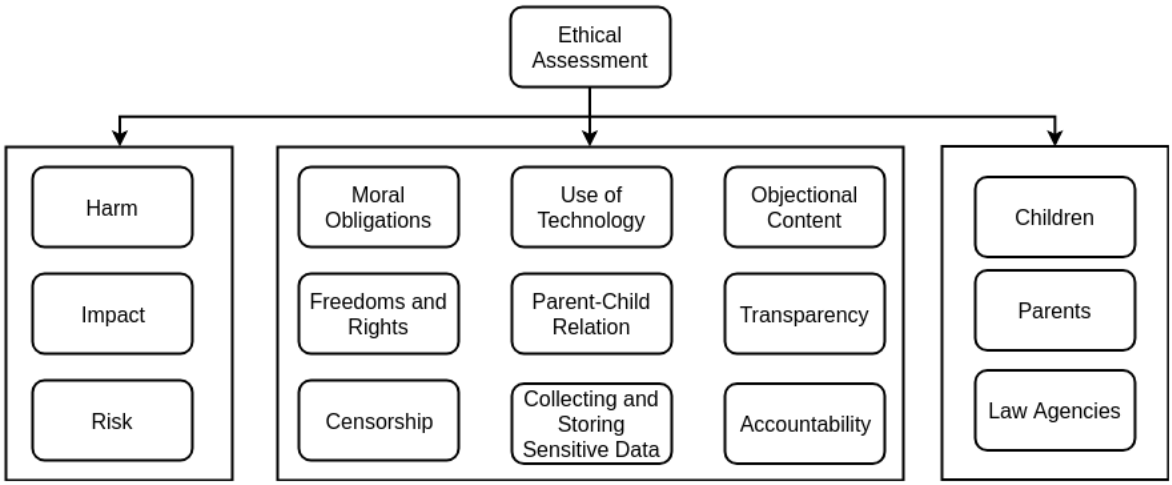
The right to not be subjected to automated decision making provides individuals the right to demand human intervention for decisions made solely by algorithms that have a significant effect. In this case, the automated detection of sensitive information by Cilter using algorithms may apply to this right, in which case, Cilter should have procedures regarding how the human intervention should be handled. However, because of the nature of information, the human intervention could be a potentially sensitive issue itself. In this case, Cilter could opt to have the human intervention by recruiting the parent of the individual as the human resource.

Data Breaches

Data breaches occur when private or secure information is potentially accessed by unauthorised entities, whether by intentional or unintentional means. Because of the sensitive nature of information stored by Cilter, a data breach has the possibility to have serious consequences, especially when the information in question contains potentially identifiable personal data. The organisational practices concerning data breaches include measures taken to minimise the risk of the breach occurring, as well as the identification and handling of a breach after it has taken place.

Minimising data breaches include adopting sufficient technological measures regarding the safety and security of data in its collection, usage, storage, and transmission. It also includes adopting organisational measures, including training of staff in the handling of personal data and information in a safe and secure manner. For example, securing the passwords and keys, and ensuring these cannot be accessed by other personnel. Procedures should be in-place and documented regarding handling of data breaches. This includes the identification of the extent of the breach, actions taken to determine affected individuals, and the notification to appropriate authorities, as well as individuals.

Ethics Assessment



While data protection laws such as the GDPR mandate some form of ethical considerations, such as through the DPIA process, it is imperative to conduct a specific and focused ethical assessment of processes apart from the data protection process. This allows detachment of data protection requirements from ethical considerations (from a social viewpoint) and allows an organisation to address moral and social issues regarding its use of technology. A suggestion is to use R&I tools such as the Ethics Canvas https://www.ethicscanvas.org/

The focus of data protection is on the data or informational aspect, whereas that of ethics assessments is on the human aspect, whether through the individual or society, or even the implied moral and social values followed by an organisation. Therefore, when conducting an ethics assessment, the focus should be on concerns and risks directed towards the organisation and how they could be handled. The underlying motivation is the establishment

of trust by imparting information regarding how Cilter fulfils the social and moral expectations, which includes identification of expectations through questions regarding risks and practices.

In its mission, Cilter inherently has a focus on the ethical and moral aspects of technology associated with children. Therefore, the focal point of individuals affected by Cilter are and will be the children who use its services. Additionally, social concerns and expectations regarding children are far greater than those for adults, particularly when it comes to harm. In order to address these, Cilter should lay out its understanding of the concern, and provide information on how addresses them. The intended audience of this information may not necessarily be the individuals who use the service, and may not understand the provided technical explanations. One way to address this is the use of simple language to explain the motivation behind the technology or process and how it addresses the specific concern. For example, in addressing how data will be kept safe, the use of encryption can be accompanied with additional information in the form of explanation regarding how encryption in general prevents unauthorised use of data.

The underlying principle of an ethics assessment is to understand the impact of the technology or service on the individual, to investigate whether the individual has provision of all required information and rights, and to assess whether a process, though legally compliant, might impact the individual in unexpected ways.

Summary

Data Protection

The focus of a data protection framework is on the assessment of practices surrounding the collection, use, storage, and sharing of personal data. In this regard, laws (in differing jurisdictions) have different requirements and definitions in terms of what constitutes as personal data, and the regulations which dictate its use.

The questions and recommendations stated in the document enable identifying and structuring information associated with the processing of personal data. These include the personal data in question, its purpose of processing, the categories of processing it undergoes, its possible storage and sharing with recipients, and the legal basis which justifies these activities. Structuring the information in this manner also provides transparency in addition to the documentation for legal compliance. Anonymisation, specifically, needs to be documented and evaluated with respect to sufficient guarantees regarding the possible re-identification of individuals and the intent of further use for anonymised data.

In addition, the protection of information also carries with it the necessity to establish and use several technical and organisational measures. These include technical measures pertaining to the security of data - such as access control and encryption, but also include information about the storage of data - such as its location, medium, technology used.

Where a service provider or device is used for these, the documentation of technical measures should include the capabilities and guarantees afforded by that specific technology. Organisational measures include safeguarding through the adoption of policies and codes of conduct which establish procedures for normal as well as critical operations, and the prevention and handling of risks and crisis as and when they can occur.

The documentation is structured in the form of sections addressing each of these topics through a brief discussion and a recommendation where possible. The intent is to use these as a template for ex-ante as well as ex-post documentation of this information.

Ethical Assessment

The focus of ethical assessments is to go beyond the requirements dictated by law, though some laws such as the GDPR also incorporate a certain degree of such ethical assessment in their requirements for compliance. In particular, ethical assessments must focus on the affected individuals (or groups or society) and balance their freedoms and rights against the intent of the activities to be undertaken. With this regard, the assessment should revolve around the notion of risks, harm, and impact on the individual.

By identifying risks and impact, it is possible to address them where possible, or to make the individual aware regarding what has been addressed. The best way to incorporate this is to adopt it as a necessary process along with data protection impact assessments in the course of service development and operation. The questions provided in the Ethical Assessment reflect some commonly found concerns regarding the use of technology around personal data and especially children. Addressing them requires the use of a more social approach in the use of language rather than stating the technical know-how as a solution. The aim is to build trust in the use and operation of the service rather than providing a justification.