Key Considerations for Protecting Data of Children and Minors

Summary of Key Regulations for protection of Children and Minors

Many jurisdictions around the globe have had legislation that aims to protect the rights and personal data of children and minors for decades. More recently many have updated their privacy legislation to focus on protecting children and minors online. These laws are often divided into two main categories.

- The first type is legislation that defines the rights of the parent or guardian, the duties of government agencies, the duties of healthcare providers, etc. when it comes to a child or minor. Typically these laws assist in, for example, protecting the release of personal data to the media when the child or minor is not of age; the prevention of the release of personal data to parents and guardians when the child or minor comes of age; and ensuring the parent or guardian provides consent(s). Naturally this is an over simplification of these laws. They may include additional 'powers' for the parent or guardian and/or additional requirements of the government agency or health care provider. These laws also may affect enterprises that hold personal data about children and minors directly or tangentially. For example, the enterprise that provides an on-site day care might have a number of procedures in place to protect children and minors. This may include a series of permissions to parents that address what personal data and photos might/might not be released to the public or media.
- The second type of legislation focuses on those enterprises that offer products and services to children and minors, both online and offline. This includes a very narrow set of enterprises, in part because of the complexity of implementing the requirements. In the past, most enterprises that offer their products and services to adults have privacy notices that include a statement that in one way or another reads "we do not offer our services to children or minors" to avoid having to address procedures for children or minors.

Some jurisdictions have expanded their privacy legislation with a section specifically for children or minors. Some speak only to on-line services and others to both on-line and off-line. In the U.S., there is legislation specifically for children and additional requirements for children in other sector specific laws. These laws recognize that children and minors may be less aware of risks, consequences, safeguards and their rights in relation to the collection and use of their personal data. They certainly are less likely to read a privacy notice and establish their settings accordingly. This is where parental or guardian responsibility enters in and the challenges of the enterprise to create a product or service that is inviting for children or minors and yet protective as well.

Both types of laws contain the same elements as legislation written for adults, but add in additional language around specific personal data such as photos and the contents of email; verifiable parental



consent; privacy settings controlled by the parent or guardian; required background checks for employees; guidance for chat rooms and pen-pals; passive tracking; etc.

Guidance for children and minors also comes from the privacy and data protection regulators in the form of proactive advice or fines of specific enterprises for wrong doing. This is especially true in the on-line space, as products and services and their technology are changing fast. As the regulators respond to the changing environment, they are writing the playbook for protecting children and minors in real-time.

To make things more complicated, the definitions of a child, a minor and an adolescent vary from jurisdiction to jurisdiction. A child in many jurisdictions includes an individual that is 13 - 16 and under. A minor is defined in a myriad of ways upwards to 21. The definition of an adolescent also differs from jurisdiction to jurisdiction and legislation to legislation. It behooves the enterprise to collect such definitions and the legislations to which they apply to ensure that their procedures accommodate these definitions, especially if they are a global enterprise.

Steps for addressing data pertaining to children and minors

- Understand the legislation that applies to children and minors for products and services the enterprise offers:
 - a. E.g. The California Consumer Privacy Act prohibits sale of customer personal information of a consumer:
 - i. under 13 years of age, unless parental or guardian consent is obtained; and
 - ii. between 13-16 years of age, unless opt-in consent is obtained.
 - Are there any tangential programs the enterprise offers that could be impacted,
 e.g. on-site daycare, benefits programs for dependants, etc.
- Understand the regulatory risk that applies to collecting and using children and minors' personal data. Research the fines or guidance given by the relevant data protection/privacy regulators, and remain current with the emerging issues such that the enterprise may be proactive in implementing change or may work to influence alternative solutions with industry and regulators.
- Determine the key definitions of a child, minor and adolescent for the jurisdictions you serve:
 - a. Identify the similarities and the differences.

- Create an inventory of personal data holdings:
 - a. Identify what personal data is collected, stored, used, shared, secured, trans-border flowed and retired by jurisdiction for children and minors and adolescents which purpose;
 - b. Map each legislation/jurisdiction to the inventory.
- Before making policy and notice decisions, engage the lines of business responsible for the relevant product, service and process around how to deliver a privacy and security-compliant product, service or process:
 - a. Consider establishing a dynamic cross-functional support team for those developing products and services designated for children and minors. In the fast pace development world, integrating data privacy in real time will help minimize rework and fines.
- Conduct privacy risk assessments and privacy impact assessments using the information provided by lines of business to identify and prioritize the risks to the enterprise;



- Based on the PIA and PRA, develop privacy controls to address the risks, including, e.g., special processes required for children and minors, such a verifiable parental consent or data minimization.
- If a major part of the enterprise's offerings, develop a separate policy for handling of children and minors' data based upon the above findings or update the enterprise existing data protection and privacy policies:
 - a. E.g. The California Consumer Privacy Act prohibits sale of customer personal information of a consumer:

- Implement the privacy controls and changes to policies and procedures into the operational practices. Work with the lines of business to achieve this.
- Continue to monitor for new and existing operational practices for changes needed in policies and procedures based on whether the nature or extent of data collected from children & minors changes or the legislative landscape evolves.

Do your regulatory research — better yet, let us do it.

Spending hours online searching and understanding privacy regulatory changes is time-consuming. Nymity Research does it for you, keeping you on top of the latest laws, regulations, standards, and operational best practices around privacy, across a multitude of jurisdictions.



Start your free trial