The rights of children and young people on digital platforms

Stakeholder guide

IMY. Swedish Authority for Privacy Protection

BARN OMBUDS MANNEN

Statens medieråd

This guide is produced by The Swedish Authority for Privacy Protection,
The Ombudsman for Children in Sweden and The Swedish Media Council.

FOREWORD

Protecting and reinforcing the rights of children and young people

As children and young people today increasingly live their lives in digital environments, it is of utmost importance that their freedoms and rights are safeguarded there, as much as they are protected in the physical world.

Children and young people move quickly and expertly between various platforms, but this does not always mean that they realise the risks or understand the consequences – consequences that may be far away in the future.

Regulating the internet is often difficult. The legislation is sometimes complex, the language is far from the language used normally by those affected by the legislation, and the perspectives are rarely as holistic as they may need to be, when considering an event from a child's perspective. However, these things we are obliged to do as the Convention on the Rights of the Child was incorporated into Swedish law on 1 January 2020.

Thus, we three Government Agencies in Sweden with special responsibility to protect children and young people and safeguard their rights, have decided, based on our separate areas of expertise, to jointly publish this guide.

The aim of the guide is to provide general support, primarily based on an integrity perspective (where the General Data Protection Regulation, GDPR, is a central legislation) and a child rights perspective (based on the Convention on the Rights of the Child). The guide also contains advice based on the intentions of the legislator in terms of protecting children from harmful media influence.

With this guide we primarily aim to reach stakeholders who create and operate various digital environments where children and young people regularly spend time. Whether you own or create websites, Swedish-language platforms, or have your own YouTube channel, we hope that you will find this guide useful.

We are convinced that by working together and putting the best interest of the child first, we can create safe and secure digital environments adapted to the needs of children and young people.

Stockholm

The Swedish Authority for Privacy Protection
The Ombudsman for Children in Sweden
The Swedish Media Council

Table of contents

Secure digital environments for children and young people

Sweden shall be a world leader in utilising the possibilities offered by digitalisation. That is the goal of the Government's digitalisation strategy. The digital world influences all levels of society, and as citizens we are getting used to most services being available online, whether it is contacting authorities, do our errands or completing work tasks.

For children and young people, the digitalisation of schools and the access to online units has a large impact on their everyday. According to the preschool curriculum, even younger children shall have access to digital tools. After school, many children and young people spend a large part of their spare time on streamed media, games, and social platforms.

From a child rights perspective, it is clear that digitalisation creates need for safe and secure digital environments adapted to children and young people. The Government has noted the need for digital safety in terms of reinforced security and integrity within its digitalisation strategy. The strategy underlines that private and public stakeholders must act responsibly and that secure digital systems are needed to protect personal integrity. In practice, this means that developers and users of digital tools and services must adhere to the rules in place to protect children and young people.

Hopefully this guide will help facilitate the work for those who create and are responsible for different digital environments and who wants to contribute to offer children and young people safe digital environments. This guide may be seen as a summary of considerations that need to be made according to the Convention on the Rights of the Child, the General Data Protection Regulation and children's right to be protected from harmful media influence.

The best interest of the child – according to the Convention on the Rights of the Child

Sweden adopted the UN Convention on the Rights of the Child (UNCRC) already in 1990. As of 1 January 2020, the UNCRC is also incorporated into Swedish national law. This means, that all the rights of the UNCRC can be implemented as Swedish law and that children are seen as rights holders, which gives them a stronger legal standing.

The UNCRC contains universal provisions aimed to safeguard the child's needs in terms of security, health, wellbeing, family relationships, as well as physical, psychological and emotional development, identity, freedom of speech and integrity to form their own opinions and the right to be heard. The Ombudsman for Children is a government agency responsible for representing the rights and interests of children and young people based on the UNCRC.

As a creator and person responsible for a digital environment, it is important to have knowledge of children's rights in order to ensure that children are protected and can develop in the digital environment. Out of the 54 Articles of the UNCRC, Article 3 is one of the fundamental principles that we will highlight in this guide. Article 3 determines that the best interest of the child must be considered in all measures and decisions concerning children. The UNCRC explicitly highlights the role of adults in the protection and promotion of the best interest of the child. Anyone creating services targeted to children and young people can contribute by focusing on the best interest of the child and departing from the UNCRC in all decisions relating to the offer and its design.

In order to focus on the child and maintain a child rights perspective, basic knowledge of the UNCRC is needed. The articles in the Convention are all connected and must be considered as a whole. Not all rights are relevant in all matters relating to children, but to ensure a child rights perspective, at least the four core principles of the UNCRC must be considered.

Find out more

https://www.barnombudsmannen.se/barnombudsmannen/barnkonventionen/

https://www.barnombudsmannen.se/globalassets/dokument-for-nedladdning/publikationer/en-skrift-om-barnkonventionen-uppdat.pdf

The fundamental principles of UNCRC

Article 2 – every child has the same rights and the same value

Article 3 – the best interest of the child shall be considered in all decisions relating to children

Article 6 – every child has the right to survival and development

Article 12 – every child has the right to express their opinion and to be heard

In addition to the core principles, there are a number of provisions that may be particularly relevant concerning the rights of children and young people online. In this guide, the articles relating to children's freedom of speech and information (Article 13) and the right to privacy and family life (Article 16) and the role of mass media (Article 17) are particularly relevant, as are the articles relating to physical or psychological violence (Article 19) and protection against other forms of exploitation (Article 36).

The child's rights – according to the General Data Protection Regulation

This guide describes selected parts of the requirements set out in the General Data Protection Regulation (GDPR) for when the personal data of children and young people are being processed.

GDPR and its provisions on data protection is founded in the Charter of Fundamental Rights of the European Union. The regulations are associated with the individuals' right to respect for their privacy and family life in accordance with the European Convention on Human Rights. Protection of privacy is also stipulated in Swedish constitution; in the Instrument of Government. Both the GDPR and the European Convention on Human Rights are law in Sweden. GDPR is directly applicable as law in Sweden and throughout the EU. Swedish law must not conflict with the Regulation.

The GDPR provisions are applicable throughout the EU and aim to create a uniform and equal level for the protection of personal data. There is a data protection authority in every EU country to monitor compliance with the rules. In Sweden, the authority is The Swedish Authority for Privacy Protection[1].

The General Data Protection Regulation especially highlights children, stating that *children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.*

This is reflected for example in the special provision on children which stipulates that children over the age of 16 years can consent to their personal data being processed for the use of **information society services**, such as social media or chat programs. Every member state has had the opportunity to lower the age indicated in the provision, and Sweden has decided that children over the age of 13 years can give consent in these cases.

GDPR contains a number of fundamental principles which can be said to be the core of the Regulation, and which are important to understand and implement. These principles stipulate for example that those responsible for the processing of data relating to children:

- may only collect personal data for explicitly stated and legitimate purposes.
- are not to process more personal data than is necessary for those purposes.
- are to ensure that the personal data is accurate.
- are to erase the personal data when it is no longer needed.
- are to protect the personal data, for example so that unauthorised persons are not given access to it and so that it is not lost or destroyed.
- are to be able to demonstrate that and how you live up to the General Data Protection Regulation.

1 Formerly by name The Swedish Data Protection Authority

Obligations and rights

The General Data Protection Regulation contains both **obligations** for those processing personal data and rights for the individuals whose personal data are being processed. The obligations include taking into consideration the fundamental principles outlined above. The following are some of the **rights** given to both children and adults:

- **The right to know who** is processing personal data, for what purpose and why.
- **The right to access** the personal data held by an organisation free of charge, and to receive a copy in an accessible format.
- **The right to object to** an organisation processing personal data without consent, unless there is a higher priority public interest. The right to object at any time to direct advertising, i.e. advertising sent directly to the recipient.
- **The right to have data corrected** if they are incorrect, incomplete, or untrue when they are processed by an organisation.
- **The right to have data deleted**, which is also referred to as the right to be forgotten. This right is applicable if a person's data is no longer needed or is being processed illegally. Other rights, such as the freedom of speech, must be protected. For this reason, it is not always possible to delete personal data that is displayed for example through a search engine.
- **The right to move data** relates to when personal data is being used by a company following consent or agreement. In that case, the data can be returned or transferred to another company at the individual's request. This is referred to as the right to "data portability".
- **The right to be informed of the loss of personal data** means that an organisation that holds personal data must inform The Swedish Authority for Privacy Protection about any personal data breaches that entail a risk to the privacy of an individual. If the breach poses a high risk to an individual, the individual must also be informed in person.

Remember

The terms GDPR and the General Data Protection Regulation are used synonymously in the guide and they refer to the same set of regulations.

When multiple actors are involved, for example in a service or platform, each party must take responsibility for their part in accordance with the General Data Protection Regulation and other applicable provisions.

GDPR is not applicable to the extent that it would infringe on any rights set out in Sweden's Fundamental Law on Freedom of Expression (YGL). This means that the provisions are not applicable to publication of personal data on the internet in cases referring to databases with certificates of publication and the automatically protected databases of mass media companies.

Concepts in the General Data Protection Regulation

One condition to be able to implement the General Data Protection Regulation is an understanding of what certain central concepts mean, such as data controller, data processor and data subject.

- **A data controller** is the organisation (for example a limited company, foundation, association, or authority) that determines for what purposes the personal data is processed and how it is processed. It is thus not the manager at a workplace or an employee who is the data controller. A natural person can also be a data controller, as is the case for example with sole proprietorships. In the guide, we address representatives of the data controller's organisation with reminders of what to keep in mind, etc.
- **A data processor** is an entity that processes personal data on behalf of a data controller. A data processor is never part of the data controller's organisation. A data processor may be a natural or legal person, public authority, agency, or other body. Cloud service companies and other external suppliers of IT services are often used as data processors for example. A processor and its personnel may only process personal data in accordance with the instructions issued by the controller and there must be an agreement between the parties.
- **Joint controllers** is a concept where several actors jointly control and have responsibility for the same processing. They are then joint controllers.
- **The data subject** is the person whose personal data is being processed.

There are more definitions inside the guide.

Remember

The information in this guide is based on GDPR, whose provisions are applicable throughout the EU. The guide does not claim to describe all data protection rules in the world. The guide draws inspiration from a statutory code of conduct from the British data protection authority ICO (Age appropriate design: a code of practice for online services). However, it does not have the same status as the British code of conduct but shall be read as normal information from a government authority regarding the applicable rules.

Protect children from harmful media influences

How can children be protected from harmful media influence in digital environments? What does harmful media influence mean and how does it relate to the design of digital services?

The concept can be divided into several subsections, including:

- harmful media content,
- harmful communicative actions,
- harmful interaction design and
- harmful use.

The three first ones are especially important to be aware of for any person creating and being responsible for different digital services.

”Harmful media content refers to any media content that can lead to children suffering negative consequences.”

Harmful media content refers to any media content that can lead to children suffering negative consequences. This may relate to violence, horror and pornography. Such content can lead to strong feelings of fear or discomfort in the moment or to the child later on having difficulty sleeping, having nightmares or hesitating to do things they would normally do. Propaganda, advertising or media content promoting problematic beauty standards are other examples of potentially harmful media content.

Harmful communicative actions include some form of social interaction. Examples include cyberbullying, hatred, threats, virtual sexual abuse or hate speech. It may include actions primarily targeted to one or more people with directly hostile intentions or actions carried out where the perpetrator does not consider how their actions affect other people. Today, anyone with access to technology can publish content in the form of text, image, and sound. Many digital services include forums for this, such as chat functions where users can interact. User-generated media content can remain for a long time after the time of publication and it can be spread to more people than what was intended.

Harmful interaction design refers to a user experience design that leads children and young people to make choices that could be harmful to them, such as sharing sensitive personal data or personal images.

Harmful use is not the focus of the guide as it concerns the negative effects of sitting still and excessive media use, such as overweight, sleeping difficulties and strain injuries.

How are children protected?

In many areas of society, children have been deemed to have special needs of protection. Their rights must also be safeguarded. Protecting children from harmful content is one such area, since children may be less critical and therefore more receptive to various messages.

Measures to protect children from harmful media influences – in legislation and self-regulation

According to the Marketing Act, it is prohibited to send direct advertising to children under the age of 16 years and to target direct purchase prompts to minors. The Radio and Television Act contains provisions limiting content with depictions of violence and pornographic imagery. The Convention on the Rights of the Child contains provisions regarding the child's right to a safe childhood and freedom of expression. According to the data protection rules, the personal data of children (and others) must be protected. There are also codes of conduct used for example to combat online hatred, and voluntary agreements with industry stakeholders, such as ethical rules regarding special caution in marketing communications targeted to children and young people.

Protection against harmful media content

Children can be protected from harmful media content, for example through the age limits set by the Swedish Media Council for films that are screened in public and the broadcasting licences that regulate the hours of the day when certain types of content can be broadcast through linear television. The internet is not regulated in the same way, but it is important for anyone providing services where children and young people may come into contact with harmful media content to consider the UNCRC and children's rights.

Children have a special need for protection

The UNCRC is significant in keeping children from being exposed to harmful content. According to the provisions, children are entitled to search, receive and disseminate information and thoughts in all forms. But children are also entitled to protection from information that can be harmful to them, and to protection against invasion of privacy and anything that can be detrimental to the child's integrity or reputation. Children also have the right to special protection of their privacy and their personal data, especially when it comes to targeted advertising or collection of data from services targeted specifically to children.

The Audiovisual Media Services Directive (AVMSD)

Implemented in Sweden primarily through the Radio and Television Act, with provisions regarding broadcast television and video on demand. The provisions relate, among other things, to the design of advertising, the quantity and placement of adverts, protection of minors and provisions relating to content that incites hatred. The Directive has recently been adjusted, which requires changes in the Radio and Television Act that are essential to stakeholders responsible for digital platforms. A new chapter relating to video sharing platforms will be introduced in the Act. Requirements are set for suppliers of a video sharing platform to take suitable measures; user-generated videos, television programmes or audio visual commercial messages with detailed and realistic depictions of violence or pornographic images must not be offered in a manner that entails a considerable risk of children seeing them, unless justifiable for special reasons. The supplier must also take measures to ensure that such videos, television programmes and messages do not have the content referred to in the provisions of the Penal Code relating to unlawful threats, instigation of rebellion, agitation against an ethnic or national group, unlawful depiction of violence and child pornography offence. The new provisions are proposed to enter into force on 1 December 2020.

Varying levels of maturity

When deciding which content is harmful, consideration is given to the emotional and intellectual maturity of children, which develops continuously. The older a child becomes, the greater is the child's ability to handle and relate to the content it's faced with. Children's ability to assess risks and understand consequences of their actions is also something that develops over time. Younger children may for example lack the tools required to handle frightening media content or to understand the consequences of publishing images or sharing personal data. The degree of protection is thus impacted by what the target group looks like and by the different ages and maturity levels of children.

"Children's risk of exposure is thus also a factor that needs to be considered when creating digital environments where there are children present. "

More vulnerable than others

Some children are at greater risk than others of being affected by harmful media influence. Children with neuropsychiatric impairments will generally use media more frequently than average. They also state to a greater extent that they have been subjected to threats, online bullying or someone being mean to them online.

Children with intellectual disabilities also report to a greater extent that someone has been mean to them on the internet. Children's risk of exposure is thus also a factor that needs to be considered when creating digital environments where there are children present.

Examples of government agencies working with this field

The Swedish Media Council

The Swedish Consumer Agency

The Swedish Press and Broadcasting Authority

Office of the Chancellor of Justice

The Swedish Police Authority

Checklist – the guide in brief

- Let the UNCRC and the best interest of the child permeate your service!
- Remember some important concepts! **Personal data** include more than just names and addresses – it is all information that can be linked to an individual.
- For what purposes do you need to process personal data? The purposes determine which data you are allowed to collect, how long they can be saved and whether you are allowed to share the data with others.
- You may never use personal data unless you comply with the General Data Protection Regulation (GDPR)! Consent and agreement are examples of legal grounds that can make it permissible to process personal data.
- GDPR-proof your consents! Consent must be given as a clear expression of will, without coercion and with the possibility of revoking it at any time.
- Provide information about how children's personal data will be used. The information must be **adapted to children** if they are the target group.
- Conduct a **risk assessment** before collecting the personal data! This is a legal requirement and helps you plan the measures you need to take in order to protect the personal data.
- Be prepared to manage the rights of individuals in accordance with the General Data Protection Regulation, such as requests for access and erasure.
- Process as few personal data as possible and consider privacy aspects and child protection in the planning and design of services and systems.
- Counteract threats and hatred on your platforms and protect children from harmful media influences.

CHAPTER 2

1. What is required to process names, images and other personal data?

Consent is not always required – but is sometimes necessary

A common misconception is that you always need a person's consent to publish or otherwise process their personal data. That is not the case. What is always required in accordance with the General Data Protection Regulation, however, is some form of legal basis. Processing personal data without a legal basis is forbidden. If you want to process personal data, you therefore need to find a provision in the regulation (a legal basis) that provides support for what you intend to do, otherwise the processing is illegal. If there is no other legal basis that works in the context, consent may be the only alternative. The consent must also meet a number of criteria in order to be legally valid, such as being informed, voluntary and revocable. In this context, it may be worth remembering that children are not always considered old enough to give consent.

Information

Find out more about how the legal basis of **consent** is legally used in section two, page 22. There is also information about the age where children can start making decisions regarding their personal data.

Personal data and personal data processing

Personal data is any kind of information that can be linked to a living person. This might for example be your name, address and personal identity number. Photos of people are also classified as personal data. In fact, even sound recordings that are stored digitally can constitute personal data even if no names are mentioned in the recording. A corporate identity number is not personal data, unless it is a one-person company. A car's registration number may constitute personal data if it can be linked to a natural person. Personal data processing is everything you do with personal data: collection, saving, sharing, sorting, publishing and so on.

The legal bases

Below we list the legal bases that **privately operated** organisations primarily use.

Consent
Can be used under certain circumstances as a legal basis for personal data processing.

Contract
Can be used as a legal basis to process children's personal data if necessary in order to fulfil the undertakings of a contract. A contract can only be used if the child is old enough to be able to control their personal data in the individual case.

Legal obligation
Laws or regulations mean that it is sometimes necessary to process certain personal data in your operation.

Balance of interests
Means that the data controller considers whether the organisation's interests outweigh those of the individual and whether the processing can be deemed necessary for the controller's present purpose. If the answer is yes, the processing is allowed pursuant to the legal basis of a balance of interests. Contracts and legal obligation are also used as legal bases by **public operations**, such as government authorities. For public operations, personal data may also be processed as part of a public interest and exercise of official authority (the most common legal basis for public operations). Consent and balance of interests can normally not be used as legal bases in public operations.

Information
Find out more in section two, page 20, about the conditions for consent, children's possibilities to give consent, and when minors are in control of their own personal data.

Keep in mind – when selecting a legal basis

Why do you need to process personal data? The purposes set the limits for what you are allowed to do and determine which legal basis is appropriate.

The General Data Protection Regulation requires you to specify the purposes. The reason is that it is not okay to collect more personal data than what is needed for the concrete purposes that have been identified.

It may be necessary to apply different legal bases for different purposes. Using personal data to deliver a product to a customer and to send advertising to that customer are examples of two different purposes.

Consent is normally not the easiest nor the most appropriate alternative, for example because the person who gives their consent can revoke it at any time. If that happens, the personal data processing must cease.

Is there a contract in place?

Consent is not usually required when there is a contract with a person. In the case of an online purchase, for example, the customer expects to have their product delivered. For the product to be delivered, the store needs to use certain personal data, such as the customer's address. The information necessary to fulfil the contract may thus be processed using the contract as the legal basis. If the operation wishes to use personal data for purposes other than fulfilment of the contract, such as sending advertising, the customer must give their consent.

Balance of interests

If there is no contract in place and it is difficult to use consent, it is normally possible to use a balance of interests, which is the most flexible legal basis of all. It requires the intended personal data processing to be **necessary** to fulfil a purpose relating to a **legitimate interest**, and that the **individual's interest in having their personal data protected does not outweigh** the legitimate interest of the operation.

So which operational interests are legitimate? This includes processing of personal data that is absolutely necessary to prevent fraud, but also processing of personal data for direct marketing can be considered a legitimate interest. Even if there is a legitimate interest, you must assess whether the intended personal data processing is necessary in order to fulfil the legitimate interest. If you make the assessment that you can use the balance of interests, you also need to ensure that the protection of privacy does not outweigh your interests in the individual case. The answer is determined by what impact the personal data processing will have on the person's privacy. In summary, a balance of interests usually works when the persons whose personal data you intend to process expect a certain kind of personal data processing.

That children need special protection is an important component to consider in the balance of interests. If you are able to show that within the planned processing you can protect the personal data of the children, provide sufficient information and otherwise safeguard the children's privacy, this impacts on your possibility to legally use their personal data pursuant to a balance of interests.

Which interest weighs heavier?

In order to determine which interest weighs heavier, a child impact analysis can be carried out. The analysis must show the consequences and effects that different courses of action could entail.

- How are children affected by different courses of action?
- What are the consequences for children in vulnerable situations? Is there a great risk of their rights being violated or that their rights cannot be fully safeguarded?

Remember

- Children are individuals living in varying circumstances.
- Take into account age and maturity.
- Your choice of legal basis must be documented. Among other reasons because the individuals whose information is being processed are entitled to know the legal basis.
- The legal basis shall be decided before the personal data is collected.

Online publication

If the information published online contains personal data, a legal basis is required as for any other personal data processing. In some cases, it is evident that consent is required, for example when the data relates to a child with protected identity. The appropriate legal basis for online publication is determined by the context, for example how sensitive the data referred to is. If you are uncertain of how to consider a publication in the sense of GDPR, it is always wise to ask the individuals concerned for their consent. In case of typically harmless publications, in contexts where many individuals are involved, such as a company's images from a mingling event, it can often be more appropriate to base the personal data processing on a balance of interests. Remember that images and other personal data relating to children are always considered worthy of special protection. Children may have more difficulty predicting the risks of sharing their data and understanding what rights they have in terms of protection for their data.

In some cases, the provisions of GDPR do not apply to online publications, even if they contain personal data. Generally speaking, GDPR is not applicable to constitutionally protected publications. The website of a journal, and in some circumstances its webcasts, **are automatically protected under the constitution**. Examples of constitutionally protected websites are aftonbladet.se and dn.se. Others whose databases are not subject to automatic constitutional protection can apply for a **publishing certificate** that provides them with corresponding constitutional protection for their websites. Examples of websites with constitutional protection through a publishing certificate are eniro.se and hitta.se.

If you have a platform that is not fully covered by the data protection regulations due to constitutional protection, there are other applicable rules. The person who runs the constitutionally protected operation is obligated to appoint and report a **responsible editor** to the Swedish Press and Broadcasting Authority. The publisher is legally responsible if **a freedom of expression offence** is committed, for example agitation against an ethnic or national group, slander or insult. Furthermore, the **act on responsibility for electronic bulletin boards (1998:112)** contains requirements for those who own or are responsible for a site. The person who provides the service must remove any posts that contains agitation against an ethnic or national group, instigation of rebellion, child pornography offences and copyright infringement.

Who is responsible for the legal basis when several actors are involved?

In all operation types (such as services and platforms) where several actors are involved, it is important that all parties are aware of their respective responsibility for the personal data processing that occurs. Several parties can be simultaneously responsible. As soon as you have access to personal data, you must ask yourself: What responsibility do we have for this information? It is important that you investigate whether you have responsibilities as a data controller or a data processor. The meaning of these terms was explained in chapter one.

As a data controller operation, keep in mind the following legal requirements:

- You must ensure that the processing is carried out in accordance with all the provisions of the General Data Protection Regulation.
- You can transfer the actual processing of personal data (for example the practical work involved in a service, the management of your customer register, etc.), but the data controller responsibility can never be transferred.
- You must conclude a data processor agreement with the data processor.

If you are in the role of data processor, keep in mind the following legal requirements:

- You are only allowed to process personal data as instructed by the data controller and you may not hire another data processor without prior written permission from the data controller.
- Some requirements set for the data controller also apply to you, such as keeping records of your processing, ensuring an appropriate level of security and in some cases appointing a data protection officer.

The data controller and the data processor can be subject to supervision or administrative fines and they can be liable for damages.

This guide primarily targets actors whose target group is children, but it can be good to know that **guardians (and all private individuals)** also have a responsibility for personal data being processed by them. If you process personal data under the management of an operation, for example in your work, your employer is the data controller or processor. Parents of children who are old enough to control their own personal data need to have a legal basis for their processing of their child's (or other person's) personal data.

Remember that processing of personal data that is covered by the **exemption for purely personal or household** activity is not subject to GDPR. This refers to processing of personal data that a natural person carries out as part of an activity that is of a purely personal nature or which relates to their household. However, the exception does not apply when a private individual publishes personal data in a manner that makes the personal data available to an indefinable number of people, for example by publication online. In that case, you must always comply with the provisions of GDPR.

Information

Find out more about parental control in section eleven, page 40.

Find out more

Advice on how to weigh interests and information about all the legal bases
https://www.imy.se/lagar--regler/dataskyddsforordningen/rattslig-grund/intresseavvagning/

What does public interest and exercise of official authority mean?
https://www.imy.se/lagar--regler/dataskyddsforordningen/rattslig-grund/myndighetsutovning-och-uppgifter-av-allmant-intresse/

What happens when you use the legal basis of contract for online services – see the guide issued by the joint data protection authorities
https://www.imy.se/globalassets/dokument/eu/avtal-som-rattslig-grund-vid-anvandning-av-onlinetjanster.pdf

How to conduct a child consequence analysis
https://www.barnombudsmannen.se/barnombudsmannen/publikationer/genomfora-barnkonventionen/provning-av-barnets-basta/

What rules apply to personal data processing in public operations?
https://www.imy.se/

Measures that The Swedish Authority for Privacy Protectioncan use against anyone who violates or is at risk of violating the rules
https://www.imy.se/om-oss/arbetssatt/tillsyn/vad-kan-tillsynen-leda-till/

2. The possibility of giving consent

Are children and young people in control of their own personal data?

In accordance with the data protection regulations, **children over the age of 13 years** can consent to their personal data being processed when using **information society services**. Examples of such services are social media, blogs, internet forums, video sharing platforms, chat programs, online games, apps with games or other content.

There is no specified age limit set in GDPR for when a child is able to consent to personal data being processed in other situations.

Age and maturity are factored in

How to approach this? When it comes to **children under the age of 13 years**, the guardian's consent must always be obtained. The parents have the main responsibility for the child's upbringing and development based on what is considered to be in the child's best interests. **Children over the age of 16 years** generally have a certain right to act independently in society and can for example dispose of their own earnings. A person who has turned 16 years old should normally also be able to give valid consent to the processing of personal data.

But what applies to **children between the ages of 13 and 16 years**? The answer is that it needs to be assessed in each individual situation if the child in question can be considered able to understand the consequences of consent. Factors influencing this assessment include how sensitive the personal data provided by the child are, how long they will be saved, as well as the age and maturity of the child.

You must consider whether the child is able to predict the potential consequences of the personal data processing and whether the child is able to understand what they are consenting to. The age limit needs to be balanced between the right to be included and the risk of the child being harmed. It is important to consider the right of each child in relation to this risk. The child is entitled to receive information adapted to age and maturity as well as the right to express his/her opinion and to be included in measures and decisions that impact the child's life.

"The age limit needs to be balanced between the right to be included and the risk of the child being harmed."

Even if the ability to understand more complex information and understand the consequences of their actions develops continuously with age, there are large individual differences. Some children may need more support to

understand the consequences for example of providing their personal data, than what could be expected based on their chronological age. This applies in particular for children with special needs, for example children with intellectual disabilities.

Since the age of children and young people have such a large impact on the possibility of allowing them to give legal consent, it may in some cases be necessary to carry out age checks.

Adapt information for children

How do we create information adapted for children and how do we ensure that the information reaches the child when the parent needs to give consent? By adapting the information to the recipient, we are better able to ensure that the information reaches the target. When adapting information to children, it is important to remember the following:

- Use clear language.
- Keep the text short.
- If a guardian needs to provide consent, it must be stated clearly early in the text that the child concerned is entitled to the information.
- Children live in different circumstances. Does the information need to be available in other languages or does it need to be read out loud?

It can sometimes be difficult to know if the information is adapted to children. One way to handle this is to let a group composed by children participate in the production of a text.

Information

Find out more about age verification in section seven, page 35.

Remember

- Regardless of whether valid consent has been provided by children or adults, the personal data processing need to live up to the rest of the rules of the General Data Protection Regulation, for example in regard to the right to information about how data is processed and adequate data security.
- The guardian's consent is not required for preventive or advisory services offered directly to children. The reason for this is that children should be able to seek advice or support, such as from BRIS, without their parents knowing.
- According to UNCRC, every child is entitled to express their opinion in any decisions that concerns them. The child's best interests must be taken into consideration, and the child has to be asked before anyone else gives consent to share the child's personal data.

Legal requirements for consent

Consent must be voluntary

In order for the consent to be valid, it must be provided voluntarily. This means that anyone who gives their consent has a genuinely free choice and control over their personal data. Voluntary consent can be explained through the following points:

- **Without coercion.** The data subject must not feel pressured to give consent. The consent is not valid if anyone has been coerced in conjunction to giving it. An example would be if you were forced as part of a customer club to agree to commercial mailings in order not to lose any bonus points.
- **Right of withdrawal**. A person who provides their consent must be entitled to withdraw it, which must be clearly stated. It must be just as easy to give consent and to withdraw it, otherwise it can be declared invalid. This is particularly important when it comes to young people. If the person who has given their consent is not able or allowed to withdraw it without suffering negative consequences, the consent is not voluntary. If consent is withdrawn, the data controller must cease the processing that was based on the consent.
- **Equal relationship between the person doing the processing and the person whose data is being processed.** In order for the consent to be considered voluntary, the relationship between the person processing the personal data and the person whose data is being processed must be "equal" in the sense of the data protection regulations. Consent cannot be used as a legal basis, for example in relation to pupils at a school, due to the uneven relationship between the pupils and the school. Pupils are required to go to school and they receive grades there, which means that they may not feel that they have the option to say no. This is also the reason why consent cannot generally be used as a legal basis in public operations. However, consent can be used outside of the school's regular activities, for example in school photography.

"In order for the consent to be valid, it must be provided voluntarily."

Consent must be provided for each individual purpose

The consent does not meet the requirements for voluntariness if several purposes are combined. If there are several different purposes for wanting to use personal data, you must obtain consent for each purpose separately for them to be considered voluntary and valid. If a company wishes to ask for consent partly to use their customers' personal data to send them targeted advertising, and partly to give the customers the possibility of participating in a specific contest, these are separate purposes. Forcing the customers to say yes or no to "all or nothing" is not legal.

Remember the example from the section above, regarding the online store that may need to process personal data for multiple purposes. You should then consider which legal basis is appropriate for each given purpose. If there are personal data deemed necessary to deliver products for example? In that case, the personal data processing should be included in the purchase agreement concluded with the data subject. Do not include anything in the contract that requires separate consent, but ensure that the terms of the agreement only includes what belongs in it. You may not for example condition the delivery of goods upon the person consenting to the sharing of personal data with another company, unless this is necessary to fulfil the purchase agreement.

The consent must be specified

For the young persons who consent to understand what they are saying yes to, the description of the purposes must be detailed and adapted to their age. The rule has been set in order to protect the users from processing where the person processing the information is ambiguous, hoping that they will be able to use the personal data for other purposes. This is illegal. Wordings indicating that the personal data will be used "for future commercial purposes" are not sufficiently specific for example and do not give grounds for legal consent.

The consent must be a clear expression of will

There must be no doubt that the person giving their consent has clearly approved the processing. A statement or clear confirmation from the data subject is required. This must be a conscious act. The interface must therefore contain an active choice, such as ticking a box. Already ticked boxes or other opt-out solutions, meaning solutions that require direct action from the person in order not to give their consent, are illegal. The same applies to wordings where silence or inactivity is interpreted as an active choice, such as "if you do not select an option, we assume that you consent".

Information is required when the consent is obtained

When it comes to children and young people, you must be particularly attentive to ensure that they have reached the maturity to understand and consent to the processing. Information targeted to children must be written in a clear and simple language. Remember that minors have different preconditions. What if you do not know the age of the person you are communicating with? Create a design that the youngest can understand. One basic rule for all actors who want to comply with the provisions set out in UNCRC regarding the right to participate is to respect the premise that the child must be able to understand what they are consenting to. If this premise has not been considered, the consent may be invalid. The person who collects the data has the responsibility to prove that the consent is valid. For a piece of information to be considered clear enough, it must include the following:

"You must be particularly attentive to ensure that children and young people have reached the maturity to understand and consent."

- Who is asking for consent, i.e. who you are.
- What kind of personal data are you going to process?
- For what purpose you want to use the personal data. If you have more than one purpose, describe each one separately.
- That it is possible to revoke your consent and how to do this.

A data controller must be able to show that valid consent has been obtained

The data controller must also be able to prove that they are complying with the rules and regulations. The burden of proof is on the data controller to show that a valid consent has been obtained and that the data subject has received all the relevant information. For this reason, it is necessary to document how and when the consent was obtained and which information the data subject received.

Checklist for obtaining consent

Before:

- Verify that consent is the most appropriate legal basis for processing of personal data.
- Ensure that the request for consent is clearly worded and separate from other terms and conditions.
- Avoid making consent a prerequisite for receiving a service.

Inform the recipient of:

- The name of the data controller for the service.
- The name of the data processor, if there is one.
- Name of any third party, such as another organisation that will have access to the data.
- How the child revokes their consent.
- That the child can refuse to give their consent without suffering negative consequences.

Remember in your communication:

- Explain why you want to access the data and what you intend to do with them.
- Do not use default consent, for example by having pre-ticked boxes. Consent must be an active choice.
- Use a clear and simple language that is easy to understand.
- Be specific and give clear alternatives for different purposes, ensure separate consent for each case of personal data processing. Vague or general consent is not enough.

Create order in your routines by:

- Document evidence of the consent: who, when, how and what information was provided.
- Continuously review the method of obtaining consent and update it as needed.
- Keep consent requests separate from other terms and conditions.

Be prepared if consent is withdrawn:

- Ensure that personal data can be immediately deleted.

Find out more

Guidelines from the joint data protection authorities
https://www.imy.se/globalassets/dokument/riktlinjer-om-samtycke.pdf

3. Risk assessment

Is it always a requirement to analyse the risks before processing personal data?

You must always carry out a risk assessment *before* starting any processing of personal data. This applies regardless of whether you intend to launch a new app, an online service or your own channel. Throughout the personal data processing you are also obligated to assess risks and otherwise protect and handle the data correctly.

The risk assessment determines what measures are required

The reason why a risk assessment must be made is that it determines which measures you need to take in order to protect personal data in your specific operation. You must carry out appropriate technical and organisational measures to ensure – and also prove – that the processing is carried out in accordance with data protection regulations. The measures taken must be regularly reviewed and updated as needed. Technical measures include encryption and authentication. Organisational measures can relate to meticulous procedures for those working with the data, such as ensuring that only the necessary number of people have access to the data.

”You must always carry out a risk assessment before starting any processing of personal data.”

But how do you know what measures are appropriate in the given case? This requires taking into consideration what type of personal data processing is involved, the nature of the personal data, the context and any conceivable risks in each given case. You need to consider the likelihood of an event that entails a risk to the personal data and how serious the consequences would be if that event were to occur.

One example of a risk can be if security is inadequate, allowing the “wrong” people to gain access to personal or sensitive data. It may relate to personal data that could entail a risk of discrimination, identity theft, fraud, financial loss or reputational damage. The higher the probability of a risk, the higher the level of security is required.

In addition to the risk to the individual’s privacy, your risk assessment should also consider the risk of jeopardising human rights according to the ECHR, such as the freedom of expression, freedom of thought, conscience and religion, freedom of movement and prohibition of discrimination. The special rights held by children and young people in accordance with UNCRC must also be included in your risk analysis, for example in terms of children being protected from all forms of violence and discrimination, the principle of the child’s best interests, and the right of children to express their opinion.

Impact assessment

If the risk assessment indicates that your planned personal data processing will **likely entail a high risk** of violating the freedoms and rights of individuals, GDPR requires you to carry out an **impact assessment**.

In accordance with the data protection regulations, an impact assessment is always required in the following three cases:

- Systematic and extensive assessment of personal aspects relating to natural persons, which is based on automatic processing, including profiling.
- Processing on a large scale of sensitive personal data.
- Systematic surveillance of a public space on a large scale.

Information

Read more about profiling in section twelve, page 42.

What this means in practice is clarified in The Swedish Authority for Privacy Protection's list of when to conduct an impact assessment. The list was created with the help of guidelines and criteria issued by the European Data Protection Board (EDPB). According to the list, an impact assessment must *for example* be made in the following cases:

- A company uses its customers' location data, for example obtained through a mobile app, for the purpose of targeting advertising to the customer or to plan its marketing strategies.
- A company obtains data from social media to profile natural persons and then target advertising to certain select groups. Keep in mind that it is prohibited in accordance with the Marketing Act to target advertising to children under the age of 12.
- An internet search engine collects data about individuals using the service, in order to create customer profiles and target marketing.

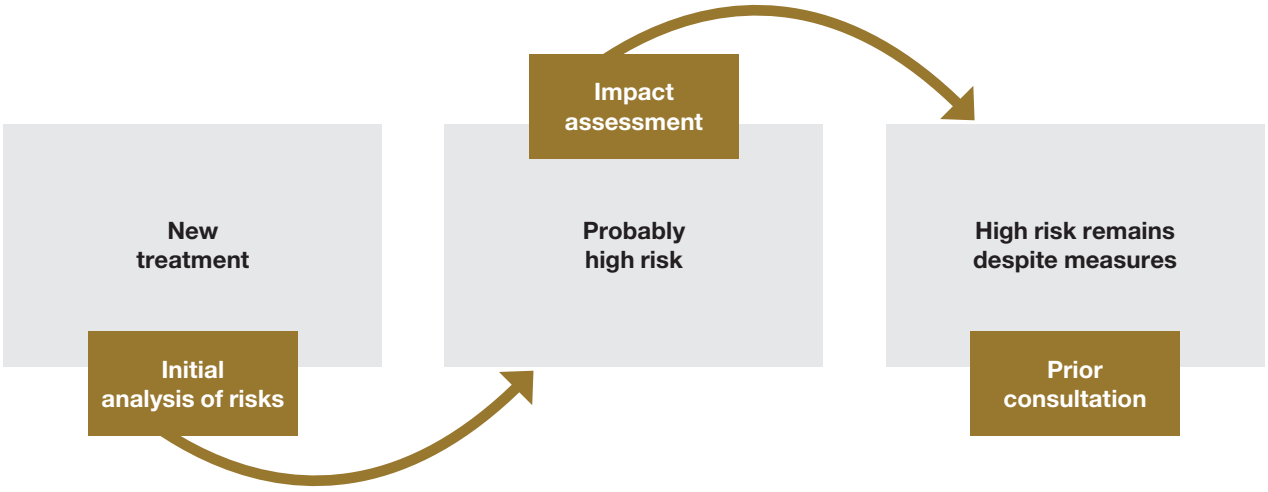
European Data Protection Board, EDPB

An independent European body contributing to the uniform implementation of the data protection rules throughout the EU/EEA. It also promotes collaboration between the data protection authorities and provides general guidelines to clarify terms and interpret the rights and obligations set out in the provisions of the GDPRR.

If the impact assessment shows that the risks cannot be adequately limited and that the risk remains high, a preliminary consultation with The Swedish Authority for Privacy Protection is required before processing begins. Such consultation requires you to have documented your impact assessment and to account for any residual risks and the reasons why these have not been possible to rectify.

The Swedish Authority for Privacy Protection has the option of prohibiting any processing that violates the GDPR. As a data controller or data processor you are as a rule to be in contact with only one member state's supervisory authority, the so-called "lead supervisory authority". To know which supervisory authority is your lead supervisory authority you need to determine where your main or only activities are carried out.

Risk assessment according to GDPR:



Information

Find out more about how a child impact assessment is carried out in section two, page 16.

Sensitive personal data

Certain personal data is by its nature particularly sensitive and therefore has stronger protection. This type of data is called sensitive personal data. Sensitive personal data is information concerning:

- ethnic origin
- political opinions
- religious or philosophical beliefs
- membership of a trade union
- health
- a person's sex life or sexual orientation
- genetic data
- biometric data that uniquely identifies a person.

Processing of sensitive personal data is generally prohibited. But there are exceptions: non-profit political, philosophical, religious or trade union organisations may process sensitive personal data regarding their members. It is also legal to process sensitive personal data if the data subjects have expressly given their consent.

Remember

There are many other types of personal data that merit special protection and which in practice may require the same security measures as sensitive personal data. These can include:

- Financial information.
- Information about a person having committed a crime.
- Valuating data, such as information from performance reviews, results of personality tests or profiles.
- Information relating to a person's private sphere.
- Information about social conditions.

Personal data breach

Is a security breach that can entail risks to a person's freedoms and rights, such as discrimination, identity theft, fraud, malicious rumours, financial loss, or breach of confidentiality or professional secrecy. A personal data breach has for example occurred if data relating to one or several data subjects has been destroyed or fallen into the wrong hands. All organisations are required to report certain types of personal data breaches to The Swedish Authority for Privacy Protection within 72 hours of the breach being discovered.

4. Requirements relating to deletion and information

How can the rights of children and young people be safeguarded during personal data processing?

Adapt the information to age

Everyone, children and adults alike, is entitled to be informed of how their personal data will be used. Informing children often requires particular care. Children can be assumed to be less aware of consequences and risks. Carefully explaining the risks entailed by a certain situation and the measures the operation has taken will help children (and their guardians) to understand the consequences of sharing their data and insight into how they can protect their personal data and privacy.

You must provide clear and concise information according to the child's age. If possible, you should provide simple diagrams, illustrations, graphics or moving material in addition to the written information, to make the information more interesting to children. If the operation's target group encompasses a large age range, a possible solution can be to create different solutions for different ages. If you choose to only have one version, you must ensure that it is accessible for everyone and understandable for the youngest target groups and people with intellectual or neuropsychiatric disabilities.

In cases where the guardian's consent is required for the personal data processing, they are primarily the ones entitled to information. However, this does not mean the child is deprived of their rights. In practice, it means that you provide both guardians and children with clear and easily available information. This can be achieved, as mentioned above, by developing different versions of the information for different target groups, or by only producing a child-friendly version.

Information requirements

The information must be free of charge, provided in an accessible format (which can be electronic) and using a clear and simple language. The General Data Protection Regulation gives detailed instructions for which information is to be provided; it must for example include contact details for the data controller, the legal basis of processing and the purpose of the processing.

The information must be provided both when the personal data are collected and at the request of the data subject. Information must also be provided to those concerned, for example if there is a data breach or similar with the data controller and there is a risk of personal data being leaked which could lead to identity theft or fraud, etc.

A reference group composed by children

When producing information adapted for children, it can be difficult to know how the information is perceived by a child. One way of ensuring that the information is correctly understood is to have a reference group of children read through and comment on the document. How do you reach children?

- Contact a school, children/youth organisation, or similar.
- Use a popup on your website with an invitation to participate.
- Send an invitation in a newsletter or similar.

At youmo.se, you can find inspiration for child-appropriate information: https://www.youmo.se/

Register extracts

The data subject is entitled to contact you in order to find out which of their personal data you are processing and in what way. You must then provide the individual with a register extract.

The register extract must contain information about which data are being processed, where the data was obtained, the purpose of the processing and the recipients or recipient categories with whom the data have been shared. The register extract must normally be provided no later than a month after receiving the request.

There may be circumstances in which information must be omitted from the register extract, for example due to other legislative provisions (such as confidentiality) or because sharing the information would be detrimental to others. The data controller should be able to clearly explain the reasons for refusing access to personal data, where applicable.

Right to erasure (“right to be forgotten”)

Both children and adults have a certain right to have their personal data erased. Even if the original collection and processing was legal, the data may have to be deleted following a request from the data subject.

When someone asks to have their data erased, you must comply in the following cases, among others:

- If the data are no longer needed for the purposes for which they were collected.
- If the processing is based on consent and the person concerned withdraws such consent.
- If the processing is carried out for the purpose of direct marketing and the person concerned does not want to be sent advertising.
- If the personal data have been processed unlawfully.
- If erasure is required in order to fulfil a legal obligation.
- If the personal data relates to a minor and was collected in conjunction with the child creating a profile in a social network.

Combatting threats and hatred

Are you looking for material on counteracting threats and hatred?

The Swedish Media Council has been commissioned by the Government to run the No Hate Speech Movement, a campaign that aims to increase awareness of racism and similar forms of hostility on the internet among children and young people.

Advice

Information material, educational tools and reports relating to the subject can be found here:

https://statensmedierad.se/nohate.1295.html

Remember

- Guardians do not need to be involved in the erasure of data, if the data subject is old enough to make the decision. Erasure must be completed immediately if the child requests it and has reached the age required to control their own data, even if the consent was originally provided by their guardian.
- If the child is old enough to give consent, you should not accept a request for deletion from a guardian without considering the child's wishes.
- It must normally be as easy for a child to delete their personal data as it is to provide them. Make it easy for children to understand what rules apply and show how they can exercise their right to be forgotten.
- The right to be forgotten does not always apply. There are certain compelling reasons that in some cases allow the data controller to keep the personal data despite the individual's objections. This may for example relate to personal data being allowed to be processed online due to freedom of expression. A search engine that receives a request for a search hit to be removed must for example weigh the person's right to privacy protection on the one hand and the internet users' right to information on the other. Circumstances indicating that a search hit should be removed include if the person is a minor or was a minor when the data was published. If a search hit results in personal attacks and mean comments, it does not necessarily mean that it must be removed, if it is also clear that these are someone's personal opinions. The context in general also matters. The information published in a discussion forum does not have the same credibility in the eyes of the public, for example, as information published in an established newspaper.

Information

Read more about at what age children can make decisions regarding their own personal data in section two, page 20.

Find out more

Guidance from the joint data protection authorities

https://www.imy.se/globalassets/dokument/riktlinjer-om-oppenhet-och-information-till-registrerade.pdf

What information is to be provided in different situations?

https://www.imy.se/lagar--regler/dataskyddsforordningen/de-registrerades-rattigheter/#information

5. Online tools

How can the tools be clarified for children and young people?

In this context, online tools mean all mechanisms used to help individuals to easily exercise their rights when they are active online.

Children and young people have their own rights, which are considered worthy of special protection. Anyone processing personal data is therefore obliged to help children and young people in particular to exercise their rights. One way of doing this is to offer online tools to download, delete, limit or correct personal data. The tools can also be used to download your own personal data or to allow users to lodge complaints.

Remember

- Make it clear to children and young people that the online tools are available. This can be done through simple icons and by highlighting the tools in the interface. As always when your target is children and young people, the information should be provided in a clear and concise manner.
- One rule of thumb is that the information must be understandable for the average member of the intended audience. It is especially important to use a clear and concise language in the information given the child's level of maturity and age.
- Keep in mind that younger children and children with disabilities may need, and are entitled to, information in an adapted format.
- Not everyone will appreciate online tools and automated processes. You must therefore also process requests received by other channels, such as e-mail and letter.

6. Saving and protecting personal data

A minimum of data

As all collection of data relating to children and young people can be considered sensitive to some extent, it is particularly important to adhere to the fundamental principle of collecting as little data as possible about this group. The principle referred to as data minimisation means that you must never process more personal data than what is required and that the personal data being processed must be clearly linked to the purpose, i.e. be relevant. Before each new processing of personal data, you must therefore consider which personal data you need as a minimum for the processing to continue.

Design for protection

Only collecting the absolutely necessary information requires you to adapt the service or system being used to collect personal data. This is referred to as privacy by default. On an online platform, this can for example mean that default settings for a social media service are set so that no more information than necessary is collected, shared or displayed.

You must take into consideration data minimisation and other privacy protection aspects already when designing an IT system and procedures. This is referred to as privacy by design, and it means that you must integrate data protection in time and incorporate it into your working methods. You must therefore design processing, products and systems in the knowledge that children are considered entitled to special protection, that they must feel safe when using services online, and that their right to privacy must be respected.

Remember

It is easier to integrate a child-friendly design into a system or product from the start than to add it later on. In this case, an impact assessment can be used as a way to more easily decide how to design the system. An impact assessment can also be helpful to detect and then assess and mitigate data protection risks for the child when it comes to personal data processing that entails a lower risk.

Information

Read more about impact assessments in section three, page 26.

Advice

This is how children can be protected from sharing data inappropriately

- Set the privacy settings on apps to ”do not share” as the standard.
- Create an extra popup window to warn the child of the consequences of a choice they are about to make.
- Design important decisions in several steps with a delay to give the child time to think.
- Include a clear, child-friendly explanation of the increased functionality and its risks when the child activates ”sharing mode”.

7. Age control

When is it appropriate to verify the user's age?

Depending on the context, it may in some cases be legal to verify user ages.

A child's age may for example have an impact on whether they are able to consent to personal data processing. Their age can also affect the risk assessment. For this reason, it may sometimes be appropriate or necessary to verify a child's age. This is only legal where there is a clear need to do so. In addition to the data protection rules, there are obligations set out in other regulations in regard to children which could mean that an age check is required. Video sharing platform providers are for example obligated to take appropriate measures to ensure that content that is harmful to children (such as realistic depictions of violence or pornographic images) are not provided in such a way that there is a significant risk that a child could see it.

There are no exact rules for how to carry out age checks, but such checks should be preceded by a risk assessment and not entail any unreasonable processing of personal data. More detailed age checks can be sensitive to a person's privacy as such. Say that a risk assessment is carried out, and the risk is considered low. It may then be sufficient to ask new users to specify their year of birth or to fill out a form where they certify that they are not children under a certain age. More detailed verification can then be carried out in case of doubt.

Information

Read more about risk assessments in section three, page 25.

The finality principle

States that personal data must not be processed later in a manner that is inconsistent with the original purposes. The principle is intended to counteract the use of collected personal data in a manner that was not specified at the time of collection.

Find out more

The fundamental principles of GDPR

https://www.imy.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/

Remember

- Consider whether it is truly necessary to verify the age of users.
- Collect as few personal data as possible.
- Do not use personal data collected for the purposes of age verification for any other purposes; this is called the finality principle.
- In addition to legislative provisions, there is self-regulation within certain industries with age limits that could have an impact on age checks. One example is PEGI, the European standard for age recommendation labels on computer games.

8. Sharing personal data with others

Is it allowed?

Sharing personal data with third parties can be allowed in some cases and in others not. The applicable rules in a specific case depend on the purpose for which the data was originally collected.

Based on what is deemed to be in the best interests of the child, consideration needs to be given to whether sharing the child's personal data is appropriate. Consideration needs to be given to the child's right to be included and to information, as well as to the child's right not to be subjected to privacy infringements. According to the data protection rules, the purpose determines whether you can share the personal data of children and young persons with third parties. You must therefore clarify why you collected the data in the first place.

Is the purpose of *sharing data* one of the **original purposes** that you informed the individual of, have a legal basis for and did you verify that this purpose otherwise meets the requirements set out in GDPR? Then the sharing is likely permitted.

Is the purpose of *sharing data* a **new purpose**? Then the sharing may be illegal.

Is the sharing of the data an original purpose?

First of all, you need to have a clear idea of why you intend to process the personal data when you begin to collect them. The purposes set the limits for what you may and may not do, for example what data you may process and for how long you may save them. The purpose determines whether you can share the personal data of children and young persons with third parties.

According to the GDPR principle regarding limitation of purposes, you are only permitted to collect personal data for specific, specified and legitimate reasons. As we have already discussed, the data subjects are entitled to information about the personal data processing. They must for example be made aware of which recipients will have access to the personal data.

If sharing the data is one of your original purposes, it is permitted if you had a legal basis for the processing when it began and you provided information to the data subjects.

Is the new purpose consistent with the original purposes?

If the sharing is a **new purpose**, you must consider the following question: Could this new purpose of sharing data be viewed as **consistent with the original purposes**? If the answer is yes, you can use the same legal basis as you did when collecting the personal data. In order to decide whether the purpose is consistent with previous purposes, it can help to consider the following:

- What kind of personal data are you going to process in the sharing? Is the data sensitive?
- What kind of processing of personal data can the data subjects reasonably expect?
- What connections are there between the purpose of the original processing of personal data and the new processing? How close is the new purpose to the purposes that the data subjects have been previously informed of?
- In what context did you collect the personal data? What relationship do the data subjects have to your operation?
- What consequences can the personal data processing have for the data subjects?
- What security measures do you have, for example authorisation control, encryption and pseudonymisation?

Information

Would you like more information about how a child impact assessment is carried out? Find out more in section two, page 16.

What do we do if the new purpose is not consistent with the original purposes?

If sharing the personal data is not compatible with the original purposes, this is an entirely new instance of personal data processing. You must then start over to find a legal basis for the personal data processing and to verify that it complies with the other provisions of GDPR.

Remember

- What is described above constitutes prerequisites for legally sharing personal data with another operation. The operation that receives personal data also needs to have a legal basis in GDPR for its processing.
- You must always inform the minor or their guardian (depending on whether the child can be said to be of an age where they can make a decision on personal data processing) that the data will be shared.
- It may be more difficult for children to fully predict the consequences of personal data being shared with third parties. It is therefore particularly important to protect children's personal data and privacy.
- More strict requirements are set for clear and easily understandable information when you address minors.

9. Using personal data for marketing purposes

Is it legal?

Under certain circumstances, it is legal to use personal data for marketing purposes. There is no absolute ban against doing so, but you must ensure that you live up to applicable regulations in this area. If you wish to use the personal data of children and young people for marketing, you must always start from what is deemed to be in the child's best interests.

Using the personal data of minors for marketing purposes can be a matter of sending advertising via email (direct advertising) or to target customised adverts to children and young people on the platforms they visit. Online marketing occurs in many formats, such as banners, advertising slots on video sharing platforms or games and other things that children frequently use. There is also marketing embedded in social media.

Before you use the personal data of children and young people for marketing purposes, GDPR requires you to:

- Carry out an impact assessment.
- Find a legal basis for processing.

The legal basis most commonly used for personal data processing for marketing purposes is the balance of interests.

Children are less aware of risks but at the same time, they deserve special protection in accordance with the rules. For this reason, it is important during a balance of interests to consider and protect the children from risks that they may not be able to assess and which they may not be aware of. This is especially true in the use of children's personal data for marketing purposes, for creating user profiles and in services targeted directly to children.

Information

Read more about the balance of interests in section one, page 15.

Find out more

https://www.konsumentverket.se/for-foretag/marknadsforing/marknadsforingslagen

Remember

- Children have the same right as adults to object to direct advertising at any time. If you receive such an objection, you must cease any mailings. You must provide information about this right in the first mailing to the minor or before you start processing the personal data. There must be procedures developed to cease this type of mailing.
- In addition to the data protection rules and the UNCRC, there are other rules to keep in mind for anyone wanting to direct marketing to children and young people. The Swedish Consumer Agency has developed a useful guidance about the provisions set out in the Marketing Act relating to advertising targeted to children and young people. These provisions also do not forbid the targeting of online marketing to children, but there are certain rules to consider:
  – The Marketing Act prohibits direct advertising to children under the age of 16 years.
  – A child must be able to understand what is advertising and what is not. For this reason, advertising must not be designed in the form of a game or similar. Nor may advertising be embedded into online games so that a child cannot distinguish the advertising from the game.

10. Geolocation data

Is it allowed to use data that reveals the location of children and young people?

What is in the child's best interests can vary from situation to situation, but as a main rule data specifying the location of children and young people must not be used.

Geolocation data (location data) can be information regarding the geographical position of a mobile phone or a tablet at a given time. Location data can make it possible to make far-reaching conclusions regarding the private lives of those the data relate to, such as their habits, where they live, the places they visit, their movements, activities and social relationships.

Location data are considered highly sensitive in terms of privacy. In general, the risks of privacy infringement increase with the amount of data and the degree of precision, as they enable a more detailed mapping of the person. Specific data, such as the exact present location of a child, can be sensitive in the sense of the data protection regulations. If a piece of data for example relates to regular visits to a clinic, conclusions can be drawn regarding the person's health, which is information to be considered sensitive and requires a separate legal basis.

In addition to the data protection aspects, the possibility of tracing a child's location entails a risk of the data being abused and thus jeopardize the child's physical safety. A permanent sharing of their location can also mean that the child's sense of personal space is limited, which jeopardises their rights. The right to privacy means that children must not be controlled or subjected to arbitrary or unlawful infringements on their personal and family lives.

Remember

- When it comes to children and young people, the fundamental principle should be that **location data is not processed**, unless there are compelling reasons to do so and the child's best interests have been taken into consideration. As in any personal data processing, the use of location data requires a legal basis in the provisions of GDPR.
- Carry out an impact assessment, consider the legal bases, ensure adequate data security and provide information to the data subjects.
- Make children and young people aware of when location data is collected, for example by displaying clear symbols. The technology can in itself make it difficult for underage users to understand when personal data is collected and which consequences this may have.
- Do not store data for longer than necessary, and use methods to anonymise the personal data to the greatest extent possible.
- In addition to the data protection regulations, there are special provisions in the Electronic Communications Act regarding location data from apps and mobile networks. The Swedish Post and Telecom Authority (PTS) is the supervisory authority in these matters.

Find out more

Swedish Post and Telecom Authority
pts.se/

11. Parental control

Tools for parental control refer to various digital solutions that give parents or guardians the possibility to limit or control what children and young people can do online. This may refer to limitations in access to the internet but also to which services or apps that can be used, which websites can be visited or amount limitations for purchases in apps. There are also tools to monitor what children and young people do online, or where they are located.

Guardians must take the child's wishes into consideration

In accordance with the UNCRC, the child's right to privacy must be respected. Tools for parental control may therefore only be used if the child is able to understand that they are being monitored and how.

Children must not be controlled or subjected to arbitrary or unlawful infringements on their personal and family lives. Guardians have the main responsibility for the child's upbringing and development based on what is considered to be in the child's best interests. In this context, parents have the difficult task of balancing interests, and this is important to be aware of. In accordance with both the Children and Parents Code and the UNCRC, parents are obliged to protect their children. They also have extensive authority to make decisions regarding the child. As the child grows older and develops, guardians must increasingly consider the child's opinions and wishes. The older the child is, the greater consideration must be given to the child's own will and consent. Guardians who use tools for parental control must take this into consideration. Parents must therefore talk to their children, tell them what the various tools are used for and consider the child's opinion before starting to use a tool. In this respect, the parent must also consider the child's right to privacy in order to determine which tools to use, how and when. It is important that guardians carry out a nuanced assessment before a tool is used, and that they talk to the child about the tool, for example in terms of why they intend to use it.

Pros and cons of parental control

These tools are important as they can be used to support adults in safeguarding and promoting the child's best interests. However, this type of monitoring can also have a negative impact on children's freedoms and rights. It can limit their possibilities of a personal life, play, freedom of association as well as access to information and freedom of speech, which in turn can affect the child's development of their own identity.

There is also a risk of the tools lulling guardians into a false sense of security. When it comes to content filters, for example, it is very difficult, even impossible, to develop technologies that filters just the right content. In practice, the filters remove too little or too much, which creates various problems. A filter that does not remove enough content can mean that the guardian lets their guard down in the belief that the filter solution has made the internet a safe space for the child. In reality, not everything is filtered out and the child may be exposed to unwanted content.

A filter that removes too much content is equally problematic. Say that the user believes that they have installed a filter to stop pornographic content, which in reality prevents access to serious sex education sites. Excessive blocking has proven to be the most detrimental to those who usually have the most difficulty finding information offline, such as young LGBTQ persons.

Children and young people can also get around the filters by going online at friend's house or in other contexts where the guardians' rules do not apply.

Information relating to the challenges of content filters should be given to the users. The recommended method is to talk to the children, who are otherwise at risk of having to deal with their experiences alone.

Inform the child

If you offer tools for parental control, you should give the child age-appropriate information about those tools. This can be done through symbols or icons indicating to the child when the monitoring is happening.

It is also valuable in this context to provide parents with information regarding the child's right to privacy. Furthermore, you need to adhere to the GDPR provisions on legal basis, security, risk assessment, information, etc. like in any use of services and tools in which personal data are processed.

Information

Read more about different parties' responsibilities according to the data protection rules in section one, page 7.

Remember

- Everyone is responsible for their own processing of personal data; this includes providers of a tool for parental control, guardians and other users.
- If you are providing content filters, you should inform your users of the risks involved in using such a tool.

12. Profiling

Can the personal data of children and young people be used to categorise individuals?

Children and adults are equally entitled not to be affected by decisions that are based solely on automated decision-making in which profiling has been part of the process. This relates to when the decision can have a large impact for the individual.

When it comes to other types of profiling where there is no automated decision-making involved, there are no specific provisions in GDPR. When you want to use profiling relating to children, you must still adhere to all rules, just like in any other personal data processing. The assessment of which legal basis that is relevant for a profiling depends, as always, on the purposes for processing.

If the profiling is necessary in order to provide a service, it may be possible to use the service agreement as a legal basis. Profiling for the sole purpose of protecting children could be founded on the legal basis of balancing interests, considering what is assumed to be in the child's best interests. Consent is often required for profiling, as it is considered highly sensitive in terms of privacy and in most situations, it is difficult to justify profiling in terms of the UNCRC and the data protection rules.

What is profiling?

Means any form of automated processing of personal data where a data amount is compiled and analysed in order to assess certain personal qualities, in particular to analyse or predict the person's health, personal preferences, interests, dependability, behaviour, place of residence or relocations, etc.

About cookies

Many websites create small files with information about their visitors and store these in the visitor's browser. These files are called cookies, and they are often necessary for profiling. As a rule, the use of cookies requires consent. This is regulated in the Electronic Communications Act, for which the Swedish Post and Telecom Authority is the supervisory authority.

Find out more

Swedish Post and Telecom Authority
pts.se/

13. Nudging

Is it allowed to use design in order to influence the choices made by children and young people?

Digital nudging is a term often used to describe how a website can steer the choices of users through the design of the experience. By giving the users a nudge in a certain direction, it is possible to control their behaviour almost unnoticed. Depending on the purpose for which this design technique is used, it is allowed to influence the choices of children and young people by design. It may be a case of illegal nudging if the child essentially has no, or only limited, options to relatively simply make considered choices.

In a situation where the choice is to say yes or no to certain personal data processing, for example, nudging can be carried out by having the "yes" alternative be a large green button and the "no" alternative written in small, illegible text. Another example is to simplify a certain choice by offering one alternative as a simple click and the other through a complicated process of multiple clicks.

When nudging is in violation of the rules

GDPR does not prohibit nudging, but it is generally inconsistent with the principle of accuracy and transparency set out in the data protection rules. Children and young people are entitled to information that is adapted to their age and maturity so that they can make informed decisions. It is important to counteract processes that are misleading for children.

Using nudging in a process intended to obtain consent to processing can for example invalidate the consent given. By using nudging, we risk jeopardising the requirement for consent to be informed and given through a clear expression of will.

Nudging can also be problematic in the use of preset age options. This can lead children and young people to give incorrect information of their age. It is therefore not recommended.

Information

Read more about consent and the age at which children can give it in section two, page 20.

Remember

The design technology as such is not usually the problem, but how it is used. Nudging can be used in ways that are fully consistent with the principles of data protection and the rights of children and young people, when it is used to steer users towards the alternative that gives them the strongest privacy protection.

The principle of accuracy and transparency

Means that, according to GDPR, the processing of personal data must be clear and understandable to the data subjects and must not be carried out in hidden or manipulated ways. Information about the processing must be easily accessible and be worded in clear, simple language.

14. Connected toys

What rules apply to the devices that collect data?

Already before a device is purchased and installed, it must be easy to understand whether it is connected to the internet, and in what way it collects personal data. When it comes to toys, it is even more important that the information is simple and clear.

Games and toys are an area that is not traditionally associated with the collection of personal data. On the contrary, play is usually an exploratory and experimenting activity where the child can test different ideas, roles and whims in a safe environment. It is therefore especially important that information about data collection in these contexts is presented in a way that is easy for the child to understand.

Examples of connected toys and devices (internet of things)

Connected toys and devices refers to physical products that are supported by functions provided through digital connection.

- These may include stuffed animals that the child can talk to, where the child is being recorded. Data in the form of audio recordings are transmitted to servers, analysed by machine and generates instructions for customised answers that are sent back and played. The child may perceive this as a conversation with their toy, and thereby be lured into sharing potentially sensitive information.
- Another example is activity bands that continuously register potentially sensitive data regarding the child's physical activity and transmits such data to servers where they are compiled, stored and used to be displayed as activity reports in an app.
- Another example are voice assistants installed in the user's home. These speakers capture voice commands and are able to communicate information from the internet to the user, for example reading news and weather forecasts, scheduling services or ordering products. At the same time, the speakers can collect a large amount of data that the users had no intention of sharing. If the speakers become part of our everyday media, the awareness of the ongoing data collection may decrease.

Well-conceived user information

It is essential for suppliers of these connected products and services to ensure that children, young people and their guardians receive the information they are entitled to. It is important to consider how connected devices function and at which times it is most suitable to communicate certain information to the child or the guardian.

Information upon purchase

Clear information that the product processes personal data must be provided to the user when they purchase the product and before installation. This can be done both on the packaging of the physical product and in the user instructions, for example using an icon showing that the product is connected to the internet and processes the user's personal data. Potential buyers should be able to read the product privacy policy, terms of use and other relevant and adapted information online without first having to purchase and install the product.

Information upon installation

The installation process for the connected toy or product is a good opportunity to give information about how the service works, how personal data is used and the consequences thereof, especially if the installation is carried out through a screen-based interface. This is especially important if the child's continued use of the product is not screen-based, as this can limit the possibilities of continuously transmitting information to the child.

Who is responsible for what?

Different actors can contribute different parts when supplying a connected device. For this reason it is important to finalise the matter of who is the data controller or data processor, and for which parts of the personal data processing each party is responsible.

Your respective obligations vary depending on your roles. If you hire another company (a data processor) to assist you in providing the service, you have a general responsibility as the data controller. This involves making sure that the data processor also adheres to the rules. The product must have appropriate security features to reduce risks including unauthorised access to the data or the product being hacked to find out the child's location.

Information

Read more about the roles of data controller and data processor on page 9.

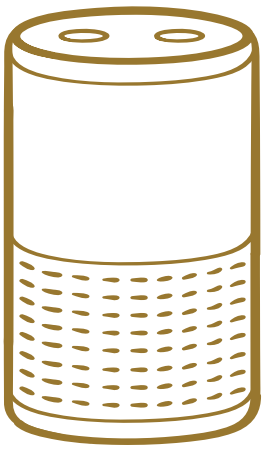
Find out more

www.barnombudsmannen.se/barnombudsmannen/barnkonventionen/

www.barnombudsmannen.se/globalassets/dokument-for-nedladdning/publikationer/en-skrift-om-barnkonventionen-uppdat.pdf

Keep in mind when designing connected toys

- Make the standard settings privacy-friendly.
- Avoid passive collection of personal data and clearly show when the device is collecting personal data. This could entail a light coming on when the device is recording images and sound or otherwise collecting personal data.
- It should be easy to turn off the collection mode on the device, for example by placing an ”offline” button directly on the device or by providing online functions to do so. It should be possible to use the toy or device to the greatest extent possible without connecting to the internet.
- A connected device may come to be simultaneously used by users of different ages. This applies especially to smart speakers and voice assistants intended to be placed in the home, which may come to process personal data regarding multiple household members and visitors. Connected toys can be used by many as they can be lent to others or used by several children playing together. Services and products should therefore be adapted for use by all of these groups. When it comes to smart speakers, it may be appropriate to enable the creation of different user profiles, which can be adapted to the user's age.



Advice

Set up a reference group of children

You can set up a reference group of children when designing a new toy. You will then be able to find out if the target group children really understand when data is being collected and when it is not.

Find out more

The Ombudsman for Children in Sweden

www.barnombudsmannen.se/barnombudsmannen/barnkonventionen/konventionstexten/

www.barnombudsmannen.se/globalassets/dokument-for-nedladdning/publikationer/allmanna-kommentarer/ak-20-svenska-formaterad.pdf

www.barnombudsmannen.se/globalassets/dokument-for-nedladdning/ak14_2019.pdf

Children's Rights in Society

www.bris.se/for-vuxna-om-barn/vanliga-amnen/unga-och-internet/barnets-vardag-pa-natet/

Council of Europe

https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

Friends

https://friends.se/friendsrapporten-2020/

Save the Children

https://www.raddabarnen.se/rad-och-kunskap/foralder/skydda-ditt-barn-fran-att-raka-illa-ut-pa-natet/

Safe surfing

surfalugnt.se/

The EU Code of Conduct

ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

This guide is produced by The Swedish Authority for Privacy Protection, The Ombudsman for Children in Sweden and The Swedish Media Council. This stakeholder guide is a translation of the original guide in Swedish. In case of a discrepancy, the Swedish original will prevail.

IMY. Swedish Authority for Privacy Protection

BARN OMBUDS MANNEN

Statens medieråd