

Applications

Children and the GDPR

Children

At a glance

- Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
- If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If you are relying on consent as your lawful basis for processing, when offering an online service directly to a child, in the UK only children aged 13 or over are able provide their own consent.
- For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
- Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
- You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
- You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

Checklists

General

- We comply with all the requirements of the GDPR, not just those specifically relating to children and included in this checklist.
- We design our processing with children in mind from the outset, and use a data protection by design and by default approach.
- We make sure that our processing is fair and complies with the data protection principles.
- As a matter of good practice, we use DPIAs to help us assess and mitigate the risks to children.

- If our processing is likely to result in a high risk to the rights and freedom of children then we always do a DPIA.
- As a matter of good practice, we take children's views into account when designing our processing.

Bases for processing a child's personal data

- When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance of power in the relationship between us.
- When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what they are agreeing to, and to enter into a contract.
- When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

Offering an information Society Service (ISS) directly to a child, on the basis of consent

- If we decide not to offer our ISS (online service) directly to children, then we mitigate the risk of them gaining access, using measures that are proportionate to the risks inherent in the processing.
- When offering ISS to UK children on the basis of consent, we make reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.
- When offering ISS to UK children on the basis of consent, we obtain parental consent to the processing for children who are under the age of 13, and make reasonable efforts (taking into account the available technology and risks inherent in the processing) to verify that the person providing consent holds parental responsibility for the child.
- When targeting wider European markets we comply with the age limits applicable in each Member State.
- We regularly review available age verification and parental responsibility verification mechanisms to ensure we are using appropriate current technology to reduce risk in the processing of children's personal data.
- We don't seek parental consent when offering online preventive or counselling services to a child.

Marketing

- When considering targeting marketing at children we take into account their reduced ability to recognise and critically assess the purposes behind the processing and the potential consequences of providing their personal data.
- We take into account sector specific guidance on marketing, such as that issued by the Advertising Standards Authority, to make sure that children's personal data is not used in a way that might lead to their exploitation.
- We stop processing a child's personal data for the purposes of direct marketing if they ask us to.
- We comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).

Solely automated decision making (including profiling)

- We don't usually use children's personal data to make solely automated decisions about them if these will have a legal, or similarly significant effect upon them.
- If we do use children's personal data to make such decisions then we make sure that one of the exceptions in Article 22(2) applies and that suitable, child appropriate, measures are in place to safeguard the child's rights, freedoms and legitimate interests.
- In the context of behavioural advertising, when deciding whether a solely automated decision has a similarly significant effect upon a child, we take into account: the choices and behaviours that we are seeking to influence; the way in which these might affect the child; and the child's increased vulnerability to this form of advertising; using wider evidence on these matters to support our assessment.
- We stop any profiling of a child that is related to direct marketing if they ask us to.

Data Sharing

- We follow the approach in the ICO's Data Sharing Code of Practice.

Privacy notices

- Our privacy notices are clear, and presented in plain, age-appropriate language.
- We use child friendly ways of presenting privacy information, such as: diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols.
- We explain to children why we require the personal data we have asked for, and what we will do with it, in a way which they can understand.
- As a matter of good practice, we explain the risks inherent in the processing, and how we intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.
- We tell children what rights they have over their personal data in language they can understand.

The child's data protection rights

- We design the processes by which a child can exercise their data protection rights with the child in mind, and make them easy for children to access and understand.
- We allow competent children to exercise their own data protection rights.
- If our original processing was based on consent provided when the individual was a child, then we comply with requests for erasure whenever we can.
- We design our processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.

Further reading

We have published detailed guidance on [children and the GDPR](#).

About this guidance	8
What's new?	9
What should our general approach to processing children's personal data be?	11
What do we need to consider when choosing a basis for processing children's personal data?	15
What are the rules about an ISS and consent?	22
What if we want to target children with marketing?	28
What if we want to profile children or make automated decisions about them?	30
What about data-sharing and children's personal data?	35
How do the exemptions apply to children's personal data?	36
How does the right to be informed apply to children?	37
What rights do children have?	40
How does the right to erasure apply to children?	43

About this guidance

These pages sit alongside our [Guide to the GDPR](#) and provide more detailed, practical guidance for UK organisations who are processing children's personal data under the GDPR.

This guidance focuses on the additional, child specific considerations. You must also read the [Guide to GDPR](#) for the requirements that apply to all data subjects.

When we refer to a child we mean anyone under the age of 18. This is in accordance with the UN Convention on the Rights of the Child which defines a child as everyone under 18 unless, "under the law applicable to the child, majority is attained earlier" (Office of the High Commissioner for Human Rights, 1989). The UK has ratified this convention.

When we refer to someone with parental responsibility for a child we mean someone who, according to the law in the child's country of residence, has the legal rights and responsibilities for a child that are normally afforded to parents. This will not always be a child's 'natural parents' and parental responsibility can be held by more than one natural or legal person.

The GDPR contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in plain clear language that they can understand. Transparency and accountability are important where children's data is concerned and this is especially relevant when they are accessing online services. However, in all circumstances you need to carefully consider the level of protection you are giving that data.

This guidance will help you understand the child specific considerations you need to think about when deciding on your lawful basis for processing a child's personal data.

It will help you understand what you need to do when you offer an information society service (ISS) to a child and process their personal data on the basis of consent, and what you need to consider if you are thinking about marketing or profiling children.

It also explains what you need to include in your privacy notices, and what rights children have under the GDPR.

For an introduction to the key themes and provisions of the GDPR, you should refer to the [Guide to the GDPR](#). You can navigate back to the Guide at any time using the link at the top of this page. Links to other relevant guidance and sources of further information are also provided throughout.

When downloading this guidance, the corresponding content from the Guide to the GDPR will also be included so you will have all the relevant information on this topic.

What's new?

In detail

- [What has remained the same?](#)
- [What's new regarding children?](#)

What has remained the same?

The GDPR does not represent a fundamental change to many of the rights that children have over their personal data. The Data Protection Act 1998 (The 1998 Act) does not specifically mention children however its provisions apply to them as individuals in their own right. For example, children have the right to request a copy of their personal data under both pieces of legislation and have the right to request that you stop processing their data. Unlike the GDPR, the 1998 Act does not explicitly require that children's data is protected and does not require that privacy notices must be clear and accessible to a child or tailored specifically for them. However, you may well have already adopted procedures that comply with these requirements as a matter of good practice.

Fairness and compliance with data protection principles remain key concepts under the GDPR and should still be central to all your processing.

The concept of competence (the child's capacity to understand the implications of their decisions) remains as valid under the GDPR as under the 1998 Act. If a child is not competent to exercise their own data protection rights or consent to processing themselves then it will usually be in their best interests to allow an individual with parental responsibility to act on their behalf. If a child is competent then your overriding consideration should still be what is in their best interests however, in most cases it should be appropriate to let the child act for themselves.

You may have processed a child's personal data applying the 'legitimate interests' condition for processing under the 1998 Act and, unless you are a public authority, this is an equally valid basis for processing under the GDPR. Public authorities now need to consider whether the processing is necessary in the performance of a task carried out for their functions or if one of the other Article 6 bases for processing applies.

We already advise data controllers to adopt a privacy by design approach, and to take into consideration the rights and freedoms of the particular data subjects whose personal data they are processing when designing new systems and processes. Data controllers who have adopted this approach for children should find they have already implemented many of the specific requirements of the GDPR.

However, it is recommended that you review any processing you undertake to ensure that it is compliant with the new GDPR requirements set out in this guidance and the Guide to GDPR, as there are some new requirements particularly about online processing.

What's new regarding children?

The GDPR explicitly states that children's personal data merits specific protection.

It also introduces new requirements for the online processing of a child's personal data.

In circumstances where an ISS is offered directly to a child, and you rely on consent as your basis for processing, in the UK only children aged 13 or over are able to give their own consent. For children under this age, unless the ISS is an online preventive or counselling service, consent needs to be provided by the holder of parental responsibility over the child.

This means that if you make your ISS available to children, and you wish to rely on consent to legitimise your processing, you need to verify that anyone providing their own consent is old enough to do so.

You are also required to make reasonable efforts (using available technology) in these circumstances to verify that consent provided on behalf of a child under the age of 13 has, in fact, been provided by the holder of parental responsibility for that child.

The GDPR also states explicitly that specific protection is required where children's personal data is used for marketing purposes or creating personality or user profiles. So you need to take particular care in these circumstances.

The GDPR says that you should not subject children to decisions based solely on automated processing (including profiling) if these have a legal or similarly significant effect on them. Although there are exceptions to this prohibition they only apply if suitable measures are in place to protect the rights, freedoms and legitimate interests of the child, and Recital 71 to the GDPR gives a clear indication that they should not be the norm. So if you currently make these types of decisions about children you need to carefully review this processing.

Finally, the GDPR requires the provision of age-appropriate privacy notices for children, and says that the right to have personal data erased is particularly relevant when processing is based upon the consent of a child.

These issues are discussed further within this guidance:

- What should our general approach to processing children's personal data be?
- What do we need to think about when choosing a basis for processing children's personal data?
- What are the rules about ISS and consent?
- What if we want to target marketing at children?
- What if we want to profile children or make automated decisions about them?
- How does the right to be informed apply to children?
- What rights do children have?
- How does the right to erasure apply to children?

Further Reading

 [Key provisions in the GDPR - See Articles 6\(1\), 8, 12\(1\), and Recitals 38, 58, 65, 71, 75](#) 

External link

What should our general approach to processing children's personal data be?

In detail

- [Why do children merit specific protection?](#)
- [What do we need to do about data protection by design and default?](#)
- [How important are fairness and the data protection principles?](#)
- [What about the best interests of the child?](#)
- [What if we're not sure whether our data subjects are children or not?](#)
- [Should we consult with children?](#)

Why do children merit specific protection?

Recital 38 of the GDPR states that:



“Children require 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. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.”

What do we need to do about data protection by design and default?

The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'. This means you have to integrate data protection into your processing activities and business practices, from the design stage right through the lifecycle.

If you process children's personal data then you should think about the need to provide the specific protection required by Recital 38 from the outset and design your processing, products and systems with this mind. This is vital if you regularly or systematically process children's personal data. It is usually easier to incorporate child friendly design into a system or product as part of your initial design brief than to try and add it in later. We recommend that you use a Data Protection Impact Assessment (DPIA) to help you with this, and to assess and mitigate data protection risks to the child. You should also take into account the rights and freedoms of the child so that their freedom to learn, develop and explore (particularly in an online context) is only restricted when this is proportionate.

If your processing is likely to result in a high risk to the rights and freedoms of children then you must

do a DPIA. The ICO has produced guidance on processing that it considers to be likely to result in a high risk to data subjects and therefore requires a DPIA. The list includes the use of children's personal data for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children. This does not mean that this type of processing will always result in a high risk to children's rights and freedom, you may not know that until after you have completed your DPIA. Rather it is the type of processing where we think there is a likelihood that the processing will be high risk. For further information about DPIAs please see our [Guide to the GDPR](#) and our detailed guidance on [Data Protection Impact Assessments](#)

Transparency is also key. You can raise children's (and their parents') awareness of data protection risks, consequences, safeguards and rights by:

- telling them what you are doing with their personal data;
- being open about the risks and safeguards involved; and
- letting them know what to do if they are unhappy.

This will also help them make informed decisions about what personal data they wish to share.

Your approach should be privacy by design and by default, taking into account the age of the children as far as you can, and the personal data you will be processing. For example, to protect children from sharing data inappropriately you could set privacy settings on Apps to 'not to share' by default, and when activating 'sharing mode' include a clear, child friendly explanation of the increased functionality and its risks.

In the context of online processing, Section 123 of the Data Protection Act 2018 requires the Commissioner to produce a Code of Practice on age appropriate design for ISS that process personal data and are likely to be accessed by children. Once published this Code will provide further guidance about the standards and practice the Commissioner will expect in this area.

Further reading

Read our sections on data protection by design and DPIAs in the [Guide to the GDPR](#).

We have also produced more detailed [guidance on DPIAs](#), including a [list of processing activities that require you to do a DPIA](#), as well as a [template](#) you can use.

How important are fairness and the data protection principles?

As with any other processing, fairness and compliance with the data protection principles should lie at the heart of all your processing of children's personal data. The purpose of these principles is to protect the interests of the individuals and this is particularly important where children are concerned. They apply to everything you do with personal data (except where you are entitled to rely upon an exemption) and are key to complying with the GDPR. The data protection principles are set out at Article 5 of the GDPR and explained further in the [Guide to the GDPR](#). For further information about exemptions please see the section of this guidance on [How do the exemptions apply to children's personal data?](#)

What about the best interests of the child?

The concept of the best interests of the child comes from Article 3 of the United Nations Convention on the Rights of the Child. Although it is not specifically referenced in the GDPR it is something that the Commissioner will take into account when considering compliance, and that you should consider when making decisions about the processing of children’s personal data. It states that:



‘In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.’

What if we’re not sure whether our data subjects are children or not?

This can be an issue, particularly with online or other remote processing. If you aren’t sure whether your data subjects are children, or what age range they fall into, then you usually need to adopt a cautious and risk based approach. This may mean:

- designing your processing so that it provides sufficient protection for children;
- putting in place proportionate measures to prevent or deter children from providing their personal data;
- taking appropriate actions to enforce any age restrictions you have set; or
- implementing up-front age verification systems.

The choice of solutions may vary depending upon the risks inherent in the processing, the rights and freedoms of the child, and the particular provisions of the GDPR that apply to your processing. You should always think about both the target age range for your processing and the potential for children outside this age range providing their personal data.

Should we consult with children?

It is good practice to invite the views of children themselves when you are designing your processing, including diverse groups who can provide a range of feedback. This can help you to identify risks, design safeguards and assess understanding, as well as giving you an opportunity to test your system or product on the end user.

It is also consistent with the UN Convention on the rights of the child which provides at Article 12 that every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.

UNICEF (The United Nations Children’s Fund) recommends that companies seek to take account of the views of children by consulting experts and child’s rights advocates and employing expert third-party facilitators with skills in engaging children according to their evolving capacities. Employing an expert facilitator can help to ensure children’s safety throughout a consultation and accurately capture children’s views and experiences.

Children in Scotland have produced some guidelines to assist organisations wishing to engage with children.

Further Reading

 [Key provisions in the GDPR - See Articles 8, 12\(1\), 25 and Recitals 38, 58](#) 

External link

Further reading

[UN Convention on the rights of the child](#)

[Committee on the Right of the Child General Comment no.14 on the right of the child to have his or her best interest taken as a primary consideration](#)

[UNICEF – Stakeholder Engagement on Children’s Rights, Part III : How to Consult Children Directly](#)

[Children in Scotland - The Participation and engagement of Children and Young People: Our principles and guidelines](#)

What do we need to consider when choosing a basis for processing children's personal data?

In detail

- [What are the lawful bases for processing?](#)
- [What if we're relying on consent?](#)
- [What if we're relying on 'performance of a contract'?](#)
- [What if we're relying on 'legitimate interests'?](#)
- [What if we're relying on 'legal obligation'?](#)
- [What if we're relying on 'vital interests'?](#)
- [What if we're relying on public task?](#)
- [What if we're processing special categories of personal data?](#)

What are the lawful bases for processing?

Before you start processing the personal data of any individual, you need to consider your basis for processing to help ensure it is lawful. The possible lawful bases for processing are outlined in Article 6 of the GDPR.

For the full list and further explanation on choosing a basis for processing, please see our [Guide to the GDPR](#) and our [Lawful basis interactive guidance tool](#)

You may rely on any of the bases given in Article 6 as your lawful basis for processing a child's personal data. However, for some of the bases there are some important additional considerations that you need to take into account when your data subject is a child.

Further Reading

 [Key provisions in the GDPR - See Articles 6 and 9](#) 

External link

What if we're relying on consent?

The GDPR allows you to process personal data on the basis of consent. For further information on this basis for processing please see our [Guide to GDPR](#) and our detailed [GDPR consent guidance](#).



“the data subject has given consent to the processing of his or her personal data for one or more specific purposes”

- Article 6(1)(a)

There may be circumstances in which you wish to process a child’s personal data using consent as your lawful basis for processing. This may be appropriate if you are truly able to give children (or their parents) informed choice and control over how you use their personal data. However consent shouldn’t be used as a way of avoiding your own responsibility for assessing the risks inherent in the processing. Although consent is a lawful basis for processing children’s personal data, using it does not necessarily guarantee that the processing is fair, and it isn’t always the most appropriate basis.

Our [GDPR consent guidance](#) provides details about the various requirements for valid consent, and you need to meet all of these. In addition, you need to consider the competence of the child (whether they have the capacity to understand the implications of the collection and processing of their personal data). If they do have this capacity then they are considered competent to give their own consent to the processing, unless it is evident that they are acting against their own best interests.

You should also take into account any imbalance of power in your relationship with the child, to ensure that if you accept their consent it is freely given.

Where the child is not competent then, in data protection terms, their consent is not ‘informed’ and it therefore isn’t valid. If you wish to rely upon consent in this situation, you need the consent of a person with parental authority over that child, unless it is evident that it would be against the best interests of the child to seek such parental consent.

In England, Wales and Northern Ireland there is no set age at which a child is generally considered to be competent to provide their own consent to processing. In Scotland children aged 12 or over are presumed to be of sufficient age and maturity to provide their own consent for data protection purposes, unless the contrary is shown.

In some contexts you may be able to make an individual assessment of the competence of a child. However, if you aren’t in a position to make this kind of assessment then you should at least take into account the age of the child and the complexity of what you are expecting them to understand.

If you accept consent from a holder of parental responsibility over a child then you also need to think about how you let the child know that he or she has a right to withdraw that consent once they are competent to make such a decision. You should provide this information in any case as part of any privacy information directed at the child. We would also recommend that you include it as part of any regular reminders you send to data subjects about their privacy settings and how to update them. For further information on privacy information please see the section on [How does the right to be informed apply to children?](#) For further information on the right to withdraw consent please see the section on [What rights do children have?](#)

The GDPR also has some specific provisions about children’s consent in an online context. It seeks to recognise the difficulties of assessing competence remotely by allowing Member States to set an age at which children can give their own consent to the processing of their personal data when an ISS is

offered directly to children. The issues surrounding online consent and children are discussed in the next section: [‘What are the rules about an ISS and consent?’](#)

Further Reading

 [Key provisions in the GDPR - See Articles 6\(1\)\(a\), 7, 8, 9\(2\)\(a\) and Recital 38](#) 

External link

What if we’re relying on ‘performance of a contract’?

The GDPR gives you a lawful basis to process personal data when this is necessary to fulfil a contract you have with the data subject. For further information on this basis for processing please see our [Guide to the GDPR](#).

“

“the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract”

- Article 6(1)(b)

When you wish to enter into a contract with a child you must consider their competence to agree to the contract and understand the implications of the associated processing of their personal data.

The legal age of capacity to enter into contracts is 16 in Scotland (with some exceptions which allow contracts with children younger than this). In the rest of the UK there is no definite age at which a child is considered to have the legal capacity to enter into a contract. The basic rule is that children over the age of 7 are generally able to enter into contracts, but (with some exceptions) the contracts they make may be ‘voidable’. This means that you can’t hold the child to what they have agreed to, or enforce the terms of the contract against them – they can effectively cancel the contract at any time. If the contract is voided then you do not have a lawful basis for processing their personal data.

This applies in all circumstances, including where you are offering an ISS.

This is a complex area of law so if you are considering entering into a contract with a child, we would strongly recommend that you seek your own legal advice about the validity of the contract. This is important both so that you can ensure that your underlying business model is legally sound and because it may affect whether or not you have a lawful basis for processing their personal data. Similarly if you are thinking about allowing a parent to agree to a contract with you on behalf of a child you should again take legal advice. You should not rely upon this summary as a full explanation of the law.

Further Reading

 [Key provisions in the GDPR - See Articles 6\(1\)\(b\), 8, 9 and Recital 44, 45](#) 

External link

Further reading

What if we're relying on 'legal obligation'?



"processing is necessary for compliance with a legal obligation to which the controller is subject."

- Article 6(1)(c)

If you are relying upon legal obligation as your basis for processing a child's personal data then your basic approach should be the same as when you process an adult's personal data under this lawful basis. You need to identify the legal obligation that underpins the processing (this could be an explicit statutory obligation or a clear common law obligation) and then establish that the processing is 'necessary' to comply with that obligation. For further detail on how to apply this test please see our [Guide to the GDPR](#).

What may be different when processing children's personal data is the underlying legal obligation. This is because there are some laws which specifically concern or seek to protect children, or which apply different standards or requirements where children are concerned.

Also, when considering whether the processing is a proportionate way of achieving compliance (and therefore whether it is 'necessary') what is proportionate in relation to adults and children could differ. You need to judge this in the circumstances of your processing, taking into account the best interests of the child.

What if we're relying on 'vital interests'?



"processing is necessary in order to protect the vital interests of the data subject or of another natural person".

- Article 6(1)(d)

Again your basic approach should be the same whether your data subject is an adult or a child. In order for this lawful basis to apply the processing must be necessary to protect someone's life. Because children are more vulnerable than adults there may be a difference in what is necessary to protect the vital interests of a child and what is necessary to protect the vital interests of an adult. You need to judge this taking into account the context of your processing. For further detail about the basic test to apply please see our [Guide to the GDPR](#).

What if we're relying on 'public task'?



“processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”

- Article 6(1)(e)

You can rely on this lawful basis if your processing is necessary for your performance of a task carried out in the public interest, or in the exercise of an official authority that has been vested in you. It usually applies to the functions of public authorities, although it can sometimes be used by private organisations that exercise official authority or carry out tasks in the public interest.

Some public authority tasks are likely to involve processing children’s personal data, for example those undertaken by Children’s Services or the Family Courts. The basic test for this lawful basis is the same whether your data subjects are children or adults; you need to identify what your function or power is and make sure that the processing is necessary for this task. What is proportionate (and therefore necessary) in relation to the processing of children’s personal data may however be different to what is proportionate in relation to the processing of adults personal data and the best interests of the child should prevail. We expect controllers relying on this basis to apply their expertise and knowledge about their functions to the child specific context. For further details of how this lawful basis applies please see our [Guide to the GDPR](#).

What if we're relying on 'legitimate interests'?

The GDPR allows controllers (apart from public authorities acting in the performance of their tasks as a public authority) to process personal data under the lawful basis of legitimate interests. For further information on this basis for processing please see our [Guide to the GDPR](#).



“the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

- Article 6(1)(f)

Under this basis for processing you need to:

- identify the legitimate interest;
- show that the processing is necessary to achieve it; and
- balance this against the child’s interests, rights and freedoms.

This is sometimes referred to as doing a Legitimate Interests Assessment and the steps you need to go through are considered in more detail in the [Guide to the GDPR](#). You need to make some judgements about the nature of the processing and the potential risks it poses and take appropriate measures to safeguard against those risks.

Article 6(1)(f) places particular emphasis on the need to protect the interests and fundamental freedoms of data subjects when they are children. This recognises Recital 38 which says that children require specific protection with regard to their personal data because they may be less aware of the risks and consequences of the processing, the safeguards that could be put in place to guard against these, and the rights they have.

When using 'legitimate interests' as a lawful basis for processing children's personal data, you therefore have a responsibility to protect them from risks that they may not fully appreciate and from consequences that they may not envisage. It is up to you, not the child, to think about these issues and to identify appropriate safeguards. You should be able to demonstrate that you have sufficiently protected the rights and fundamental freedoms of the child and that you have prioritised their interests over your own when this is needed.

Using legitimate interests as your lawful basis for processing a child's personal data puts the onus on you, rather than the child (or adult acting on their behalf), to make sure that their data protection interests are adequately protected. You need to consider what the child might reasonably expect you to do with their personal data, in the context of your relationship with them.

In practice this means that if you intend to process children's personal data you need to design your processing from the outset with the child, and their increased need for protection, in mind. You should take into account the age range of the children that you are designing your processing for when doing this, as this may affect their level of understanding and the amount of protection that they need. Although there are no defined rules on this, younger children generally need more protection and have less autonomy than older children. The freedom of children to learn, develop and explore should only be restricted if this is proportionate response to the identified risks. We recommend that you use a data protection impact assessment to help you to decide this, and if the processing is likely to be high risk then you must do a DPIA. It is also good practice to consult with children as part of your design process as this may be your best method of assessing need and understanding.

Even if you aren't actively seeking to process children's personal data (for example if you are designing a product or service that is aimed at adults not children) you need to think about whether children are able or likely to access the product or service, as if they are you may end up processing children's personal data anyway. In this circumstance you need to consider the data protection risks and either put in place appropriate safeguards to protect against them or take measures appropriate to the risks involved to deter children from providing their personal data.

Similar considerations apply if you design a product for older children, but think that younger children are likely to use it.

Further Reading

 [Key provisions in the GDPR - See Article 6\(1\)\(f\), 12\(1\), 25, 35 and Recital 38, 78](#) 

External link

Further reading

Our detailed guidance on [Legitimate interests](#)

Our detailed guidance on [Data Protection Impact Assessments](#).

For further information on the existing ePrivacy rules, please see our [Guide to PECR](#).

What if we're processing special categories of personal data?

If you are processing 'special categories' of personal data, such as health data, then as well as needing a lawful basis for processing under Article 6 you also need to identify a condition for processing under Article 9 of the GDPR. This is because Article 9 prohibits the processing of this kind of personal data unless specific conditions are met.

You need to read the conditions in Article 9 in conjunction with Sections 10 and 11 and Schedule 1 of the Data Protection Act 2018. This Schedule provides the detailed circumstances in which the UK has proposed that certain Article 9 conditions will apply. They tend to apply in very specific circumstances and many of them include a necessity test. If a necessity test applies then, the protection of children's personal data may be a particular consideration when applying this test. You need to use your sector specific expertise to decide what is proportionate and in the best interests of the child. The condition for the safeguarding of children and individuals at risk has obvious relevance when processing children's personal data in a child protection context, but other conditions may equally apply when processing children's personal data.

Further detail on the conditions for processing special categories of personal data please see our [Guide to the GDPR](#). Further guidance on the detailed provisions of schedule 1 will be provided in due course.

What are the rules about an ISS and consent?

In detail

- [What do we need to do if we intend to use children's personal data to offer an online service to a child?](#)
- [What does Article 8 say?](#)
- [What is the definition of an ISS?](#)
- [When is an ISS 'offered directly to a child'?](#)
- [When does the UK age limit apply?](#)
- [What does Article 8 of the GDPR require?](#)
- [What do we have to do if we offer an ISS directly to children?](#)
- [What does 'reasonable efforts' mean?](#)
- [What about children's consent and cookies?](#)

What do we need to do if we intend to use children's personal data to offer an online service to a child?

If you intend to use children's personal data to offer an online service to a child then you must do a DPIA to establish whether your processing will result in a high risk to the rights and freedoms of your data subjects. This is because offering online services to children is one of the circumstances that the ICO considers is likely to result in such a risk. For further guidance please see our detailed guidance on [Data Protection Impact Assessments](#).

What does Article 8 say?

Article 8 of the GDPR applies where you are offering an information society service (ISS) directly to a child. It does not require you to always get consent for the processing of children's personal data in this context, but if you choose to rely on consent it sets out further conditions as follows:



"1. Where point (a) of Article 6(1) applies in relation to the offer of information society services directly to a child the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member states may provide by law for a lower age for these purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.”

What is the definition of an ISS?

The basic definition of an ISS in Article 1(1)(b) of Directive (EU) 2015/1535 is:



“any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition:

- (i) ‘at a distance’ means that the service is provided without the parties being simultaneously present;
- (ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
- (iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.”

Essentially this means that most online services are ISS, even if the ‘remuneration’ or funding of the service doesn’t come directly from the end user. For example an online gaming app or search engine that is provided free to the end user but funded via advertising still comes within the definition of an ISS.

It generally includes websites, apps, search engines, online marketplaces and online content services such as on-demand music, gaming and video services and downloads. It does not include traditional television or radio transmissions that are provided via general broadcast rather than at the request of an individual.

If you are uncertain whether your service is an ISS or not then we recommend you take your own legal advice, or refer to the following ‘further reading’ which provides more detailed clarification.

Further reading

- [Article 1\(1\) of Directive \(EU\) 2015/1535 of the European Parliament and of the Council \(1\) 2000/31/EC](#) (the Directive on electronic commerce: recital 18)
- [CJEU Judgement Ker-Optika, Dec 2010](#) (C-108/09, paragraphs 22 and 28)
- [CJEU Judgement Uber, May 2017](#) (C-434/15, paragraphs 30-37).

When is an ISS ‘offered directly to a child’?

If an ISS is only offered through an intermediary, such as a school, then it is not offered ‘directly’ to a child.

Any other ISS which explicitly states that it is for children, or has children of any age as its target audience is clearly being offered directly to a child.

The ICO also considers an ISS is offered directly to a child when it is made available to all users without any age restrictions or when any age restrictions in place allow users under the age of 18.

If an ISS is only made available to users who are aged 18 and over then it is not being offered directly to a child. However, if your ISS states that it has such an age limit then, in the event of a complaint, we may look for evidence that the limit is applied in practice, and not just in theory, when deciding whether Article 8 applies. We may consider evidence such as site content, marketing plans, systems or processes designed to limit access, and information provided to users, in this respect.

This means that you need to carefully consider your target audience, and be clear about what age group you intend to allow to access your ISS. If you decide not to offer your ISS to children then you need to consider how to mitigate the risk of them gaining access, using measures that are proportionate to the data protection risks inherent in the processing.

Because online processing of children’s personal data is likely to be high risk processing you must use a data protection impact assessment to help you in this task and to evidence and explain your approach to processing.

When does the UK age limit apply?

Article 8 of the GDPR allows Member States to decide the age at which children can consent to the processing of their personal data in the context of an ISS, at national level. The UK has set this limit at age 13, but other Member States have set different age limits.

This means that ISS providers that have an establishment anywhere within the European Union (EU) need to respect the differing age limits of the different Member States. In practice this may mean that the child needs to select, or confirm which country they are in each time they provide your ISS with their personal data, so that you know which age limit to apply. If you have an establishment anywhere in the EU the ICO expects you to respect the UK age limit when you process the personal data of UK based children. Similarly if you are a UK based ISS provider we expect you to respect other Member States’ age limits when you process the personal data of children based elsewhere in the EU.

If you are an ISS provider who does not have an establishment anywhere within the EU, but you actively seek or pursue the use of your service by European based children, we expect you to respect the UK age limit when you process the personal data of UK based children.

If you do not have an establishment anywhere in the EU and you don’t actively seek or pursue the use of your service by European based children you don’t need to meet the different Member State requirements as your processing falls outside the territorial scope of the GDPR.

What does Article 8 of the GDPR require?

In circumstances where you are offering an ISS directly to children and you wish to rely upon consent as your lawful basis for processing their personal data, Article 8 of the GDPR (as implemented in the UK)

provides that:

- only children aged 13 years and over may lawfully provide their own consent for the processing of their personal data;
- an adult with parental responsibility must provide consent for processing if the child is under 13; and
- in such cases you must make reasonable efforts, taking into consideration available technology, to verify that the person providing parental consent does, in fact, hold parental responsibility for the child.

If your ISS is an online preventive or counselling service Section 9 of the Data Protection Act 2018 provides that the Article 8 requirements do not apply and Recital 38 of the GDPR says that parental consent should not be required. This indicates that in this context either it will be in the best interests of the child to accept their own consent or that another basis for processing (such as public task or legitimate interests) may be more appropriate.

What do we have to do if we offer an ISS directly to children?

If you offer your ISS directly to children and wish to rely upon consent as your lawful basis for processing, then you have to make sure that anyone providing their own consent to the processing is old enough to do so. Although the GDPR does not contain an explicit 'age of consent' verification requirement, this is the implication of Article 8. If you do not verify this then this may result in you processing a child's personal data without valid consent. You do not have to verify the exact age of the data subject in this context: you only need to establish that they are old enough to provide their own consent.

As there is no 'reasonable efforts' qualification to obtaining valid consent, it remains a matter of fact whether you have obtained the lawful consent of someone who is able to give it for themselves or not. However, in practice, in the event of a complaint, we will consider whether you have made reasonable efforts to verify that the data subject is old enough to provide their own consent, taking into account the risks inherent in the processing and the available technology.

The GDPR also explicitly requires you to make reasonable efforts, taking into consideration the available technology, to verify that any person giving consent on behalf of a child who is too young to provide their own consent, does in fact hold parental responsibility over the child.

A data protection impact assessment should help you to decide what steps you need to take to verify age and parental responsibility. It may also help you to evidence that they are reasonable in the event of a complaint to the Commissioner.

Further Reading

 [Key provisions in the GDPR - See Article 8](#) 

External link

Further reading

Article 29 Working Party [Guidelines on consent under Regulation 2016/679, WP258](#)

What does 'reasonable efforts' mean?

This varies depending upon the risks inherent in the processing and the technology that is available.

For example, you may wish to request an email address for a child who wants to subscribe to a band's e-newsletter via a website. As long as you are only going to use the email to send the requested e-newsletter, you may consider that the risks involved in collecting this personal data are at the lower end of the risk spectrum. A reasonable effort in this circumstance might therefore entail simply asking for a declaration that the user is old enough to provide their own consent, or a declaration of parental consent and responsibility, via a tick box or email confirmation. You may consider that further checks are not reasonable (or indeed practical) and that these steps are sufficient given the low risk to the child of the proposed processing.

However, if your ISS allows individuals to post personal data via an unmonitored chat room, it becomes more risky to allow a child to participate. You therefore need to adopt more stringent means to verify the consent you've obtained. For example, you may decide to use a third party verification service - to verify that the child is old enough to provide their own consent, or to check the identity of the person claiming parental responsibility and confirm the relationship between them and the child.

The implied need to age-verify raises the issue of how you can do this remotely and in a privacy friendly way with the minimum need for collection of 'hard identifiers' such as passport scans or credit card details. Collecting excessive information is unlikely to comply with the data protection by design approach in the GDPR. There is also the additional challenge that in the UK 13-17 year olds are likely to have a more limited range of identity documents available to them than adults.

The ICO recognises that your ability to undertake age verification in order to manage consent for online processing may be dependent upon the availability of suitable technologies and age verification mechanisms in the marketplace.

You should be wary of mechanisms that involve detailed collection and retention of any individual's personal data as this raises further data protection concerns. It is preferable to use 'attribute' systems which offer a yes/no response when asked if an individual is over a given age, or if this person holds parental responsibility over the child.

If you do collect personal data for the purposes of satisfying Article 8 then you need to make sure that you process it in accordance with all the requirements of the GDPR. This includes:

- minimising the data that is collected;
- not retaining it beyond the time that it is needed; and
- adequately protecting it.

At present in the UK it may not be easy in such online circumstances for all groups of adults to prove they actually hold parental responsibility for a child. For example parental responsibility for 'looked after' children is decided by the family courts and may be officially held by a corporate body but delegated for day-to-day purposes to the person providing the care. There may also be other situations where aspects of parental responsibility are delegated to third parties for day to day practical purposes. It may therefore, be reasonable instead to accept a verification which relies upon a declaration or statement of relationship from a verified adult. For example, a verified adult providing a declaration that they are a foster carer with day to day parental responsibility for a looked after child.

How reasonable this approach is considered to be will depend on the availability of verification services in the marketplace and the ease of using them. Longer term the option of formally certified age

verification services under the GDPR may be possible. We envisage that verification will become easier over time as the technology becomes available. The 'reasonable efforts' expected will therefore change as the marketplace develops but your approach should remain the same: evaluate the risk and in the light of those risks make reasonable efforts to verify that you have valid consent.

Further Reading

 [Key provisions in the GDPR - See Articles 6\(1\)\(a\), 7, 8, 12\(1\) and Recitals 38, 58](#) 
External link

What about children's consent and cookies?

The consent requirements for cookies are defined by the Privacy and Electronic Communications Regulations 2003 rather than the GDPR and so aren't the subject of this guidance. They basically provide that either the 'user' (the person using the ISS) or the subscriber (the person who has a contract with the internet service provider) must consent to the setting of cookies and similar technologies on the equipment (desktop computer, laptop, mobile device etc) being used. This is not quite the same as consenting to the processing of personal data in GDPR terms. However, it remains the case that for consent to be valid the person providing it must understand what they are consenting to. This means that you need to take proportionate measures, taking into account the risks inherent in technology being used, to ensure that a child providing their own consent is competent to do so. Further information on what this means in practice will be provided when our guidance on cookies is updated.

Further reading

Read the [Guide to PECR](#) for more information.

What if we want to target children with marketing?

In detail

- [What do we need to do if we intend to use children's personal data for the purposes of marketing?](#)
- [Can we use children's personal data for the purposes of marketing?](#)
- [What should we consider if we want to use a child's personal data for the purposes of marketing?](#)

What do we need to do if we intend to use children's personal data for the purposes of marketing?

If you intend to use the children's personal data for marketing purposes then you must do a DPIA to establish whether your processing will result in a high risk to the rights and freedoms of your data subjects. This is because targeting marketing at children is one of the circumstances which the ICO considers is likely to result in such a risk. For further guidance please see our detailed guidance on [Data Protection Impact Assessments](#).

Can we use children's personal data for the purposes of marketing?

The GDPR states that children's personal data merits specific protection, which should in particular apply to the use of their data for marketing purposes or creating personality or user profiles.

Using children's personal data for marketing purposes can include both using personal data to send marketing messages to individual children (also known as direct marketing) and using personal data to display targeted adverts in an online context (also known as behavioural advertising).

You are not necessarily prevented from using children's personal data for marketing purposes, but you need to make sure that you meet all the requirements of the GDPR. For example, you need to ensure the processing is fair and complies with all the data protection principles. You need to have a lawful basis for processing and must explain what you are doing with their personal data in a way that they can understand. In all circumstances you need to ensure the child is specifically protected when their personal data is processed for these purposes. You should not exploit any lack of understanding or vulnerability.

Children have the same right as adults to object to the processing of their personal data for direct marketing purposes. So, if they ask you to stop processing their personal data for this purpose you need to stop doing so. You also need to tell them about their right to object, either the first time that you send them a direct marketing message, or before you send this first message. If you intend to use profiling or behavioural advertising to target children with marketing then you should also read the section of our guidance [What if I want to profile children or make automated decisions about them?](#)

If you intend to send electronic marketing messages to children then you need to comply with the Privacy and Electronic Communications Regulations 2003 and you should read our [Guide to PECR](#). In many circumstances under PECR you need to ask for consent for direct marketing, and this means that consent is the relevant basis for processing under the GDPR as well. You should note that the Directive from which these regulations are derived is currently under review and the rules may be subject to change.

What should we consider if we want to use a child's personal data for marketing purposes?

Recital 38 says that children merit specific protection when their personal data is used for the purposes of marketing because they may be less aware of the risks, consequences and safeguards concerned.

If a child gives you their personal data, such as an email address, or information about their hobbies or interests, then they may not realise that you will use it to market them, and they may not even understand what marketing is and how it works. This may lead to them receiving marketing that they do not want. If they are also unable to critically assess the content of the marketing then their lack of awareness of the consequences of providing their personal data may make them vulnerable in more significant ways. For example, they may be influenced to make unhealthy food choices, or to spend money on goods that they have no use for or cannot afford.

So, if you wish to use a child's personal data for marketing you need to think about if and how you can mitigate these risks.

Advertising standards stipulate that marketing targeted directly at or featuring children should not contain anything that is likely to result in their physical, mental or moral harm. For example, adverts must not exploit their credulity, loyalty, vulnerability or lack of experience. They must not condone or encourage poor nutritional habits or an unhealthy lifestyle in children.

It is good practice to consider sector specific guidance on marketing, such as from the Advertising Standards Authority, to make sure that you do not use children's personal data in a way that might lead to their exploitation.

Further Reading

 [Key provisions in the GDPR - See Articles 6, 12\(1\), 21 and Recitals 38, 58](#) 

External link

Further reading

For more general information on advertising regulation visit the website of CAP (Committees of advertising practice) and ASA (Advertising standards Authority) www.asa.org.uk.

For further information on the existing ePrivacy rules, please see our [Guide to PECR](#).

Our [Direct marketing guidance](#) should also remain useful, and will be updated to reference the new requirements of the GDPR.

What if we want to profile children or make automated decisions about them?

In detail

- [What do we need to do if we intend to use children’s personal data for the purposes of profiling children or making automated decisions about them?](#)
- [What does the GDPR say about solely automated decision making, profiling, and children?](#)
- [What is profiling?](#)
- [Can a child be subject to profiling?](#)
- [What does ‘produce legal effects’ and ‘or similarly significantly affects’ mean?](#)

What do we need to do if we intend to use children’s personal data for the purposes of profiling children or making automated decisions about them?

If you intend to use the children’s personal data for the purposes of profiling children or making automated decisions about them then you must do a DPIA to establish whether your processing will result in a high risk to their rights and freedoms. This is because these are circumstances which the ICO considers are likely to result in such a risk. For further guidance please see our detailed guidance on [Data Protection Impact Assessments](#).

What does the GDPR say about solely automated decision making, profiling, and children?

Article 22 of the GDPR makes no specific reference to children which means that the same basic rules apply to them as to adults. These are considered in detail in our detailed guidance on [automated decision making and profiling](#).

You should not make decisions based solely on the automated processing of their personal data (including profiling) where those decisions have a legal or similarly significant effect upon them, unless one of the following exceptions apply. The decision:

- is necessary for the performance of a contract between data subject and controller, and the controller has put in place suitable measures to safeguard the data subjects rights, freedoms and legitimate interests;
- is authorised by Union or member state law which includes suitable measures to safeguard the data subject rights, freedoms and legitimate interests;
- is based on the data subjects explicit consent, and the controller has put in place suitable measures to safeguard the data subjects rights, freedoms and legitimate interests.

If you are required to put suitable measures in place to safeguard the rights of data subjects, then these must include at least:

- the right to obtain human intervention on the part of the controller; and
- the right for the data subject to express his or her point of view and to contest the decision.

If the decision involves the processing of special categories of personal data then the exceptions that

can be relied upon to justify the processing are more limited, and the processing can only take place if:

- The decision is based on the data subject's explicit consent and suitable measures to safeguard the data subjects rights, freedoms and legitimate interests are in place; or
- The processing is necessary for reasons of substantial public interest, on the basis of Union or member state law, and suitable measures to safeguard the data subjects rights, freedoms and legitimate interests are in place.

Further Reading

 [Key provisions in the GDPR - See Articles 22 and 9\(2\)\(a\) and \(g\)](#) 

External link

However, Recital 71 says that "*such measure*" (solely automated decision-making, including profiling, with legal or similarly significant effects) "*should not concern a child*". Although this wording is not reflected in the Articles of the GDPR itself, and so cannot be taken to represent an absolute prohibition on this type of processing in relation to children, it does give a clear indication that such processing of children's personal data should not be the norm.

The need for particular protection for children in this context is also reflected in Recital 38, which says:

“

“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. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.”

Article 21 also gives data subjects, including children, an absolute right to object to profiling that is related to direct marketing.

What is profiling?

Profiling is defined in Article 4(4) of the GDPR as follows:

“

“ ‘profiling’ means any form of automated processing of personal data consisting of the use of person data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements;”

Not all decisions based solely on automated processing qualify as profiling, and not all profiling qualify as a solely automated decision for the purposes of Article 22, although there can be some overlap.

For further discussion of this please see our detailed guidance on [automated decision and profiling](#).

Can a child be subject to profiling?

The rules in Article 22 of the GDPR relate to solely automated decisions (which can include profiling) rather than to the process of profiling in itself. This means that profiling that isn't used to make decisions about particular individuals, or profiling that feeds into a wider decision making process with a human element, isn't covered by the Article 22 rules. Neither are solely automated decisions (including profiling) which don't have a legal or similarly significant effect on the data subject.

If Article 22 doesn't apply then, as long as you make sure that you give specific protection to the child in accordance with Recital 38, the GDPR does not prevent you from profiling children. However, you still need to meet all the other requirements of the GDPR, such as processing fairly, having a lawful basis for processing and providing a privacy notice which the child can understand. You should be clear about what you are doing and why and not exploit any lack of understanding or vulnerability on the part of the child.

If Article 22 does apply, then you are not prohibited from profiling children but you should pay careful attention to Recital 71 and to the [Article 29 Data Protection Working Party Guidelines on Automated Individual decision-making and Profiling for the purposes of Regulation 2016/679](#) which says that 'where possible controllers should not rely upon the exceptions in 22(2) to justify [solely automated decision making about children, with legal or similarly significant effect]'

If you do rely upon one of the exceptions in Article 22 to justify such processing you need to demonstrate that there are suitable measures in place to properly protect the interests of the children whose personal data you are processing. In accordance with Article 22(2) if you are responsible for implementing these measures (rather than them being laid down by Union or member state law) they must include at least giving children the right to obtain human intervention, and the right to give their own view and contest a decision. Depending on the circumstances you may need to do more than this. In any case you need to make the processes by which children exercise their Article 22(2) rights child friendly and easy for them to access, use and understand. And again, you still need to comply with all the other requirements of the GDPR.



You also need to tell the child that you intend to use their personal data to make automated decisions about them and explain to them, in language they can understand, the logic involved in the decision making and the significance and envisaged consequences of the processing. This is a requirement under both Articles 13 and 14 of the GDPR

If you are considering profiling children for marketing purposes then you should take into account the following comments from the [Article 29 Data Protection Working Party Guidelines on Automated Individual decision-making and Profiling for the purposes of Regulation 2016/679](#) that 'Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes. Children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising. For example, in online gaming, profiling can be used to target players that the algorithm considers are more likely to spend money on the game as well as providing more personalised adverts. The age and maturity of the child may affect their ability to understand the motivation behind this type of marketing or the consequences. Given these comments, you are expected to justify your processing, evidencing what safeguards you have put in place and

demonstrating that it appropriate to use children’s personal data in this way.

You should also note that the child’s right to object to your processing their personal data for the purposes of direct marketing extends to any profiling that is related to that direct marketing. So if the child (or someone acting on their behalf) asks you to stop profiling for this purpose, then you must do so.

Further Reading

 [Key provisions in the GDPR - See Article 6\(1\)\(a\), 6\(1\)\(f\), 8, 12\(1\), 22, 23 and Recital 71, 75](#) 
External link

What does ‘produce legal effects’ and ‘or similarly significantly affects’ mean?

This is discussed in more detail in our detailed guidance on [automated decision making and profiling](#)

A legal effect on a child is something that has an impact on their fundamental legal rights and freedoms, or affects their legal status in some way.

A decision which ‘similarly significantly affects’ a child therefore needs to have an impact on them that is equal or equivalent to affecting their fundamental legal rights and freedoms or legal status.

Decisions based upon solely automated processing of personal data are sometime used with the aim of influencing a data subject’s future choices and behaviours. For example, in the context of behavioural advertising, a profile of past browsing habits may be used to automatically display certain products to particular individuals, with the aim of influencing them to buy those products. This can be a particular issue where children are concerned because they may be more easily influenced, and less able to understand the motivation behind such processing. An EU study on [the impact of marketing through social media, online games and mobile applications on children’s behaviour](#) found that marketing practices have clear and sometimes subliminal impacts on children’s behaviour.

Whilst not every choice a child makes in response to such processing has a ‘similarly significant’ effect on them, some may. For example, solely automated processing of a child’s personal data that influences a child to make poor food choices, to the detriment of their physical health, could be said to affect them in a way that is ‘similarly significant’ to a legal effect.

If you wish to make decisions based upon the solely automated processing of children’s personal data, with the intention of influencing their choices or behaviour, you therefore need to consider what impact those choices or behaviours may have upon the child, and decide whether this amounts to a similarly significant effect. If it does reach this bar then Article 22 will apply and, in line with Recital 71 and the opinion of the Article 29 Data Protection Working Party, we would advise you to think very carefully before you proceed with the processing, and if you do go ahead, then make sure it can be justified under one of the exceptions.

Wider evidence may help you in assessing the impact of your processing. For example CAP (Committee of advertising practice) has rules banning the advertising of high fat, salt or sugar (HFSS) food or drink products in children’s media, because of its likely effect on children’s health. The rules, which apply to media targeted at under-16s, came into effect on 1 July 2017. The ban applies in traditional and online children’s media, from magazines and cinema to social media and advergames.

In general, if advertising standards prohibit or limit the marketing of certain types of products to

children, this should give you a good indication that influencing a child's choices in this area could potentially have a similarly significant effect on them. And even if the 'similarly significant effect' bar is not met, you should remember that the Article 29 Data Protection Working Party recommends that you should avoid profiling children for the purposes of marketing. So if you decide to do so you need to be able to justify your decision and demonstrate that you have protected the children whose personal data you are processing adequately.

Further Reading

 [Key provisions in the GDPR - See Article 6\(1\)\(a\), 6\(1\)\(f\), 22 and Recital 38, 71, 75](#) 

External link

Further reading

For further information on profiling please see the [Article 29 Data Protection Working Party Guidelines on Automated Individual decision-making and Profiling for the purposes of Regulation 2016/679](#).

What about data-sharing and children's personal data?

In more detail

What do we need to do if we want to share children's personal data with third parties?

If you want to share children's personal data with third parties then you need to follow the approach set out in our Data Sharing Code of Practice. Although this has been issued under the Data Protection Act 1998 its basic approach remains valid under the GDPR. In time this guidance will be updated to reflect the specific provisions of the GDPR and the Data Protection Act 2018.

We would also recommend that you carry out a DPIA to assess the risks inherent in the data sharing. If the processing falls within one of the categories the Commissioner considers to be likely to result in a high risk to the rights and freedoms of children then a DPIA is compulsory. For further guidance on DPIAs please see our Guide to the GDPR.

How do the exemptions apply to children's personal data?

In detail

- [What does the GDPR say about exemptions?](#)
- [How do we apply the exemptions when processing children's personal data?](#)

What does the GDPR say about exemptions?

Article 23 of the GDPR enables member States to introduce exemptions from the principles at Article 5, the transparency obligations and individual rights. But only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society in certain circumstances. For further detail of these circumstances please see our Guide to the GDPR.

Chapter IX of the GDPR provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities

The specific detail of the exemptions is provided in Schedule 2, 3 and 4 to the Data Protection Act 2018. For further information please see our Guide to the Data Protection Bill.

How do we apply the exemptions when processing children's personal data?

The exemptions may allow you to process children's personal data in ways which the GDPR would not otherwise allow, if certain conditions are met.

Each of the exemptions applies in a very specific set of circumstances requiring you to work your way through a specific test in each case. This is no different with children's personal data than with adult's personal data. You need to consider the exact wording of the individual exemption in question and decide if it applies to your processing.

So if you think you should be able to process children's personal data in a way that doesn't appear to be allowed by the GDPR, you should check the exemptions that are available in Article 23 and Chapter IX of the GDPR and at Schedules 2, 3 and 4 of the Data Protection Act 2018.

Further guidance on the exemptions will be added to the Guide to the GDPR once in due course.

How does the right to be informed apply to children?

In detail

- [What information should we give to children?](#)
- [How should we provide privacy information?](#)
- [What if we are relying on parental consent?](#)
- [What if the child is pre-literate?](#)

What information should we give to children?

You must provide children with the same information about what you do with their personal data as you would give to adults. In order for processing to be fair, there is the same need for transparency, as this gives an individual control and choice.

A full list of the information you must provide, which varies depending upon whether the personal data has been provided by the individual themselves or a third party, is given in our [Guide to the GDPR](#).

As one of the reasons why children require specific protection is that they may be less aware of the risks of the processing, it is also good practice, to explain the risks involved in the processing, and any safeguards you have put in place. This will help children (and their parents) understand the implications of sharing their data with you and others, so they can take informed and appropriate actions to protect themselves.

You should make your privacy notice clear and accessible and aim to educate the child about the need to protect their personal data.

Further Reading

 [Key provisions in the GDPR - See Articles 12, 13, 14 and Recital 58, 60](#) 

External link

Further reading – ICO guidance

[Privacy Notices, Transparency and Control](#)

Detailed guidance on [the right to be informed](#)

How should we provide privacy information?

You should write in a concise, clear and plain style for any information you are directing to children in a privacy notice.

It should be child-appropriate and, as far as possible addressed directly to the relevant age group. If

your target audience covers a wide age range then you could consider providing different versions of your notice for different ages. If you choose to only have one version then you need to make sure it is accessible to all and can be understood by your youngest age range.

You should present your privacy notice in a way that is appealing to a young audience. You should consider using diagrams, cartoons, graphics and videos that will attract and interest them. In an online context, you should consider the use of dashboards, layers, just-in-time notices, icons and symbols.

What if we are relying upon parental consent?

If you are relying upon parental consent then, in terms of ensuring that the consent is informed, it is the holder of parental responsibility rather than the child who needs to understand what they are consenting to. Providing them with clear privacy information should meet this requirement.

However, as has been made clear in the Transparency Guidelines issued by the Article 29 Working Party, children do not lose their rights as data subjects to transparency just because consent has been given by a holder of parental responsibility.

In practice this means that you need to give both the holder of parental responsibility and the child clear and accessible privacy information. Again you could achieve this by developing different versions for these different audiences, or by producing a child friendly version that can also be understood by parents.

This gives the consenting parent the information they need, and also help to inform and educate young children for the future and enable them to exercise their rights on their own behalf in line with their evolving capacity to do so. You could also produce something designed to be used by children and parents together to provide parents with a tool to help with the digital education of the child.

What if the child is pre-literate?

Article 29 recognises that very young or pre-literate children are, in most cases, unlikely to understand even the most basic written or non-written messages concerning transparency. In this circumstance it is obviously appropriate to provide privacy information that can be understood by the parent. However, this does not mean that the requirement to provide child friendly privacy information does not apply. The Commissioner expects controllers whose services are used by very young children to develop privacy information that can be accessed by children as and when they develop the necessary level of understanding, or in conjunction with their parents. You should ensure that this is periodically brought to the child's attention throughout your ongoing processing relationship with them (for example when providing regular reminders about privacy settings).

Further Reading

 [Key provisions in the GDPR - See Article 12\(1\) and Recital 58, 60](#) 
External link

Further reading

ICO guidance - [Privacy Notices, Transparency and control](#) (external link)

Detailed guidance on [the right to be informed](#) (external link)

[Article 29 Working Party Guidelines on transparency](#)

The UK Council for Child Internet Safety (UKCCIS) has produced guidance and collated examples of good practice with respect to online fair processing information provided to children. This can be found at:

[Child Safety Online: A practical guide for providers of social media and interactive services 2015](#)
(external link)

The Children's Commissioner has published guidance on providing [simplified terms and conditions for children](#).

What rights do children have?

In detail

- [What rights do children have?](#)
- [When may a child exercise these rights on their own behalf?](#)
- [When may a parent exercise these rights on behalf of their child?](#)
- [How does this work in practice?](#)
- [What role do child advocacy services have in representing children?](#)



What rights do children have?

Children have the same rights as adults over their personal data. These are set out in Chapter III and VIII of the GDPR and are also listed below. For more detailed information about how these rights apply to all data subjects, please refer to our [Guide to the GDPR](#). Where these provisions raise child specific issues these are covered below or elsewhere in our pages on Children and the GDPR.

All data subjects, including children have the right to:

- be provided with a transparent and clear privacy notice which explains who you are and how their data will be processed. See '[How does the right to be informed apply to children?](#)' (link);
- be given a copy of their personal data;
- have inaccurate personal data rectified and incomplete data completed;
- exercise the right to be forgotten and have personal data erased. See [How does the right to erasure apply to children?](#);
- restrict the processing in specified circumstances;
- data portability;
- object to processing carried out under the lawful bases of public task or legitimate interests, and for the purposes of direct marketing. See [What if I want to market children?](#) (link)
- not be subject to automated individual decision-making, including profiling which produces legal effects concerning him or her or similarly affects him or her; See [What if I want to make automated decisions \(including profiling\) about children?](#) (link)
- complain to the ICO or another supervisory authority;
- appeal against a decision of a supervisory authority;
- bring legal proceedings against a controller or processor; and
- claim compensation from a controller or processor for any damage suffered as a result of their non-compliance with the GDPR.

Further Reading

 [Key provisions in the GDPR - See Articles 7\(3\), 13-22, 34, 77-79, 82 and Recitals 38, 58, 65, 75](#) 
External link

When may a child exercise these rights on their own behalf?

A child may exercise the above rights on their own behalf as long as they are competent to do so. In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases. A child should not be considered to be competent if it is evident that he or she is acting against their own best interests.

If you have already decided that a child is competent to provide their own consent then it will usually be reasonable to assume they are also competent to exercise their own data protection rights.

If a child is competent then, just like an adult, they may authorise someone else to act on their behalf. This could be a parent, another adult, or a representative such as a child advocacy service, charity or solicitor.

When may a parent exercise these rights on behalf of their child?

Even if a child is too young to understand the implications of their rights, they are still their rights, rather than anyone else's such as a parent or guardian.

You should therefore only allow parents to exercise these rights on behalf of a child if the child authorises them to do so, when the child does not have sufficient understanding to exercise the rights him or herself, or when it is evident that this is in the best interests of the child.

This applies in all circumstances, including in an online context where the original consent for processing was given by the person with parental responsibility rather than the child.

How does this work in practice?

An adult with parental responsibility may seek to exercise any of the child's rights on their behalf.

If you are satisfied that the child is not competent, and that the person who has approached you holds parental responsibility for the child, then it is usually appropriate to let the holder of parental responsibility exercise the child's rights on their behalf. The exception to this is if, in the specific circumstances of the case, you have evidence that this is not in the best interests of the child.

If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or again if it is evident that this is in the best interests of the child.

What matters is whether the child is able to understand and deal with the implications of exercising their rights. So for example, does the child understand what it means to request a copy of their data and how to interpret the information they receive as a result of doing so? When considering borderline cases, you should take into account, among other things:

- where possible, the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;

- any consequences of allowing those with parental responsibility access to exercise the child’s rights. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Further Reading

 [Key provisions in the GDPR - See Article 8 and Recital 38](#) 

External link

What role do child advocacy services have in representing children?

Article 80(1) of the GDPR allows data subjects to appoint properly constituted not-for-profit bodies or organisation (which could include child advocacy services or other organisations representing the interests of children) to exercise their right to:

- bring a complaint to the ICO or another supervisory authority;
- appeal against a decision of a supervisory authority; or
- bring legal proceedings against a controller or processor.

Article 80(2) of the GDPR provides that Member States can legislate to allow such bodies or organisations to exercise these rights on behalf of data subjects without the data subjects’ authorisation.

Under the Data Protection Act 2018 the Secretary of State must review the UK’s provisions for the representation of data subjects under Article 80, including the merits of exercising the power under Article 80(2), with a particular emphasis on the needs of children in this respect.

Depending upon the outcome of this review organisations representing the interests of children may be given a formal role in representing children’s above data protection rights. Further guidance on this will be provided in due course.

Further Reading

 [Key provisions in the GDPR - See Article 80\(1\) and 80\(2\)](#) 

External link

Key provisions in the Data Protection Act 2018

Section 189

How does the right to erasure apply to children?

In detail

- [What is the right to erasure?](#)
- [What does the GDPR say about the right to erasure and children?](#)
- [What does this mean in practice?](#)

What is the right to erasure?

Article 17 of the GDPR gives both adults and children the right to have their personal data erased in some specified circumstances where, although the original collection and processing may have been compliant with the GDPR, continuing to hold their personal data against their wishes is not. It is sometimes known as the 'right to be forgotten'. The right is overridden if certain compelling reasons to retain the personal data apply, despite the individual's objections. For further detail of the circumstances in which it applies and the reasons for which it can be overridden please see our [Guide to the GDPR](#).

What does the GDPR say about the right to erasure and children?

Recital 65 of the GDPR says that the right to erasure:

“

“...is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child...”

This is consistent with the general principle at Recital 38 that children merit specific protection because they may be less aware of the risks and consequences of processing their personal data, and applies regardless of whether the consent was originally given in an online or offline context.

In addition, Article 17(1)(f) provides that one of the specific circumstances in which the right to erasure applies is when:

“

“the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).”

Further guidance on the child specific Article 8(1) provisions is given in [What are the rules about ISS and consent?](#)

What does this mean in practice?

If an individual wants you to erase personal data that they provided when they were a child, then you should comply with their wishes whenever you can. Especially if it seems likely that they gave their personal data without fully understanding the implications of doing so.

The GDPR seeks to provide a greater degree of control over their personal data for individuals and the right to erasure is part of this.

However, the right to erasure is not an absolute right, and it can be overridden in certain circumstances, including where it is necessary for exercising the right of freedom of expression and information. When considering whether the right to erasure should be overridden in this case, you should take into account that freedom of expression is itself a qualified right. It may be restricted if this is necessary for the protection of the rights of others. So effectively you need to balance the right to freedom of expression against the need to protect the rights of others.

In a situation where a data subject provided their data when they were a child, without fully understanding the implications of doing so, there will generally be an increased expectation of what may be considered 'necessary' to protect the rights of the child. So the right to erasure is more likely to prevail in this circumstance than if data was provided by an adult. This will have to be decided on a case by case basis.

There are further circumstances in which the right to erasure can be restricted. However, we do not consider these any further here as we do not think they raise any particular, child specific issues. See our [Guide to the GDPR](#) for further detail on all the circumstances in which the right to erasure does not apply.

You need to make sure that your processes for exercising the right of erasure are easy for a child to access and understand. Article 7(3) of the GDPR says that it 'shall be as easy to withdraw consent as it is to give it'. We consider that, as a matter of good practice, this general principle should also apply to any processes related to the right to erasure. So as far as possible, it should be as easy for a child to get their personal data erased as it was for them to provide it in the first place. For example, if you started processing without asking the child to provide original identity documents then it is usually disproportionate to make this a condition of erasure.

In an online context dashboards and take-down tools should be available to allow children and other users to easily delete or remove personal data.

The right to erasure does not necessarily have to be exercised by the same person as provided the original consent. If consent was originally provided by a holder of parental responsibility this does not mean that they will also have to request the erasure. If the data subject is no longer a child, or if they are now competent to exercise their rights on their own behalf then you should usually accept their request for erasure without needing to involve the parent (or holder of parental responsibility).

Similarly, if a child is competent to provide their own consent to processing and to exercise their own data protection rights you should not accept a request to erase personal data from a holder of parental responsibility without taking the wishes of the child into account.

In cases where there is a dispute between a child and their parent about whether personal data should be erased or not, or where a child wishes to have personal data erased without their parent's knowledge, then you need to consider the level of understanding of the child and also what is in their best interests. This needs to be done on a case by case basis. Similarly in cases where there is more than one holder of parental responsibility and they do not agree about whether the personal data should

be erased or not, you should take the child's views into account when appropriate and the best interests of the child should prevail.

Further Reading

 [Key provisions in the GDPR - See Article 17 and Recital 65](#) 

External link

Further reading

The ICO has published the [Delisting criteria](#) it uses under the 1998 Act when it receives requests for personal data that has been posted online to be delisted. These were jointly agreed by the ICO and other European data protection authorities.