Key data protection themes

This section of our Guide to Data Protection contains guidance on key themes and topics, explaining how the law applies in a specific context. It is for data protection officers and others who have day-to-day responsibility for data protection.

It covers the Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (UK GDPR) as it applies in the UK.

We have published guidance on children's data. We have also published guidance on political campaigning, guidance on direct marketing and guidance on AI. We are currently developing guidance on a number of key themes including national security, and various technologies. This section will expand over time as our work develops.

Each page summarises the key points you need to know, answers frequently asked questions, and contains practical checklists to help you comply.

Where relevant, we also link to detailed guidance and other resources.

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 to 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 UK 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 international markets, we comply with the age limits applicable in each country.

☐ 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.

In brief

What's new?

A child’s personal data merits particular protection under the UK GDPR.

If you rely on consent as your lawful basis for processing personal data when offering an ISS directly to children, in the UK only children aged 13 or over are able provide their own consent. You may therefore need to verify that anyone giving their own consent in these circumstances is old enough to do so. For children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling service. You must also make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

Children also merit specific protection when you are collecting their personal data and using it for marketing purposes or creating personality or user profiles.

You should not usually make decisions about children based solely on automated processing if this will have a legal or similarly significant effect on them. The circumstances in which the UK GDPR allows you to make such decisions are limited and only apply if you have suitable measures to protect the interests of the child in place.

You must write clear and age-appropriate privacy notices for children.

The right to have personal data erased is particularly relevant when the individual gave their consent to processing when they were a child.

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

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, or think that you might, then you should consider the need to protect them from the outset, and design your systems and processes with this in mind.

Fairness, and compliance with the data protection principles, should be central to all your processing of children’s personal data.

It is good practice to consider children’s views when designing your processing.

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

As with adults, you need to have a lawful basis for processing a child’s personal data and you need to decide what that basis is before you start processing. You can use any of the lawful bases for processing set out in the UK GDPR when processing children’s personal data. But for some bases there are additional things you need to think about when your data subject is a child.

If you wish to rely upon consent as your lawful basis for processing, then you need to ensure that the child can understand what they are consenting to, otherwise the consent is not 'informed' and therefore is invalid. There are also some additional rules for online consent.

If you wish to rely upon 'performance of a contract' as your lawful basis for processing, then you must consider the child's competence to agree to the contract and to understand the implications of the processing.

If you wish to rely upon legitimate interests as your lawful basis for processing you must balance your own (or a third party's) legitimate interests in processing the personal data against the interests and fundamental rights and freedoms of the child. This involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to safeguard against those risks.

What are the rules about an ISS and consent?

Consent is not the only basis for processing children's personal data in the context of an ISS.

If you rely upon consent as your lawful basis for processing personal data when offering an ISS directly to children, in the UK only children aged 13 or over can consent for themselves. You therefore need to make reasonable efforts to verify that anyone giving their own consent in this context is old enough to do so.

For children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling service. You must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

You should regularly review the steps you are taking to protect children's personal data and consider whether you are able to implement more effective verification mechanisms when obtaining consent for processing.

What if we want to target children with marketing?

Children merit specific protection when you are using their personal data for marketing purposes. You should not exploit any lack of understanding or vulnerability.

They have the same right as adults to object to you processing their personal data for direct marketing. So you must stop doing this if a child (or someone acting on their behalf) asks you to do so.

If you wish to send electronic marketing messages to children then you also need to comply with the Privacy and Electronic Communications Regulations 2003.

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

In most circumstances you should not make decisions about children that are based solely on automated processing, (including profiling) if these have a legal effect on the child, or similarly significantly affect them. If you do make such decisions you need to make sure that you put suitable measures in place to protect the rights, freedoms and legitimate interests of the child.

If you profile children then you must provide them with clear information about what you are doing with their personal data. You should not exploit any lack of understanding or vulnerability.

You should generally avoid profiling children for marketing purposes. You must respect a child's absolute right to object to profiling that is related to direct marketing, and stop doing this if they ask you to.

It is possible for behavioural advertising to 'similarly significantly affect' a child. It depends on the nature of the choices and behaviour it seeks to influence.

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

If you want to share children's personal data with third parties then you need to follow the advice in our data sharing Code of Practice. We also recommend that you do a DPIA.

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

The exemptions apply to children's personal data in the same way as they apply to adults' personal data. They may allow you to process children's personal data in ways that the UK GDPR would not otherwise allow. You need to consider and apply the specific provisions of the individual exemption.

How does the right to be informed apply to children?

You must provide children with the same information about what you do with their personal data as you give adults. It is good practice to also explain the risks inherent in the processing and the safeguards you have put in place.

You should write in a concise, clear and plain style for any information you are directing to children. It should be age-appropriate and presented in a way that appeals to a young audience.

What rights do children have?

Children have the same rights as adults over their personal data which they can exercise as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.

How does the right to erasure apply to children?

Children have the same right to have their personal data erased as adults. This right is particularly relevant when an individual originally gave their consent to processing when they were a child, without being fully aware of the risks.

One of the specified circumstances in which the right to erasure applies is when you collected the personal data of a child under the lawful basis of consent, when offering an ISS directly to a child.

It should generally be as easy for a child to exercise their right to erasure as it was for them to provide their personal data in the first place.

Further reading

We have published detailed guidance on children and the UK GDPR.

Explaining decisions made with AI

Explaining decisions made with AI

Guidance on Artificial Intelligence and data protection

...

Guidance for the use of personal data in political campaigning

.....

Direct marketing

....

Video surveillance

.