GDPR Privacy Policy (Notice) – Goodwin Martial Arts

This document details the Goodwin Martial Arts privacy policy and the layered approach to presenting the information (for illustrative purposes only)

The privacy notice documented has extensive notes linking to relevant Information Commissioner's Office GDPR Guidance.

Appendix One (ICO Checklist commentary) contains a summary of which checklist items we have included.

Appendix Two (ICO Guidance – at a glance) contains an extract from the ICO website that forms the basis for the content of this privacy notice.

Appendix Three (Lawful Basis for processing) contains an extract from the ICO website that explains the legal basis on which Goodwin Martial Arts has determined we process personal information.

Goodwin Martial Arts Privacy Policy Notice

This notice appears in full on the Goodwin Martial Arts website.

Privacy Notice

Here at Goodwin Martial Arts we take your privacy seriously. We will only use your personal information to provide the services you have requested from us. These services include: attendance at classes, gradings and, where you choose to participate, competitions and other events which we support.

Who we are

We are Goodwin Martial Arts, the registered address for which is:

28 The Gardens, Chudleigh, TQ13 0GE

Our Data Protection Officer is Mrs Tamzin Goodwin. Mrs Goodwin can be contacted at tamzingoodwin@sky.com

What personal Information do we collect and what do we do with it?

We only collect and process the personal information that you provide us with. We do not obtain additional personal information from other sources.

We do not share your data with any third party for marketing purposes.

Personal information collected by Goodwin Martial Arts includes:

- Student name
- Student gender
- Student date of birth
- Student address
- contact telephone number (student, or if under 18, that of a parent / guardian)
- contact email address (student, or if under 18, that of a parent / guardian)
- emergency contact (name)
- emergency contact telephone number
- student photograph
- student health data (where relevant)

We need this personal data to manage your time with us as a student, whether that's training, grading or competing. Unfortunately, if you don't want to provide us with this information you won't be able to become a student with Goodwin Martial Arts.

The legal bit....

To hold your personal information, the law requires us to have what is called a "legal basis" for holding and processing your details. When you come to Goodwin Martial Arts classes, you're asking us to teach you a martial art. And when you sign up for our classes you pay us each month. This is a kind of contract, and so Goodwin Martial Arts legal basis for holding your personal information is "contractual" - we hold the information to enable us to provide you with all the services we've told you about. The personal information is required to enter into a contract with Goodwin Martial Arts

Where you are under 18 years of age, we will also collect and use personal information you provide about your parent / guardian to:

- contact them about club activities including gradings, competitions, training and other club related activities.

We also ask you to provide personal information about someone we can contact in the event of an emergency.

Student Health data

When you become a student with us we ask you to tell us about any medical conditions that may be relevant in you undertaking a martial art. We only ask for this information to ensure that you are able to train with us in a safe environment where your individual needs can be recognised.

We do not share this information with anyone not involved in teaching, grading or organising and running competitions and only when relevant to ensure your wellbeing.

You'll be asked to give explicit consent for us to hold and process the information for the purpose described above.

Who we share your data with

We only share relevant personal information with other organisations ("third parties") where it is necessary to enable you to take part in the activity, including where we use a service to manage your contract with us.

UK ITF

Goodwin Martial Arts is partnered with **UK ITF**. We are required to register students with UK ITF and this is a condition of training with Goodwin Martial Arts. We only share the personal information when necessary to register you. We share your name, date of birth and nationality.

UK ITF 192 High Street, (1st Floor), West Drayton, Middlesex UB7 7BE, United Kingdom

International TaeKwon-Do Federation (ITF)

If you achieve your black belt in TaeKwon-Do we are required to register you directly with the ITF. We share your name, date of birth and nationality.

ITF 192 High Street, (1st Floor), West Drayton, Middlesex UB7 7BE, United Kingdom

How long do we hold your details for?

Goodwin Martial Arts will hold your personal information for a period depending on what our relationship with you is.

Before you're a student

When you first contact us we will ask you to provide your name, age, email address and telephone number. We hold this information whilst we help find the right class for you or your child. If you decide against joining our classes, we will hold your personal information for six months before we delete your personal information.

Sometimes our classes are full, and we can't take any more students. If you ask to join one of our classes and it is full we will ask you if you want to go on a waiting list. If you say 'yes', we will contact you if spaces become available at the class you have asked about. We will keep you on a waiting list for 2 years before we delete your personal information.

In either case, you can contact us at any time and ask us not to contact you again (this is called your Right to object). Each time we contact you we'll make sure you can let us know that you don't want to be contacted any more. If you tell us you don't want to be contacted again we'll delete your personal information. We'll do this immediately.

When you're a student

Once you become a student we hold your personal information for the whole time you are a student with us. If you leave us we will hold your personal information for a period of 7 years after you leave. If you ask us to delete your personal information we will delete what we can but we will not delete all of your data until this 7 year period has ended.

You have the right to object to our processing of your personal information and may do so at any time. However, we hold your personal information as part of our contract with you. If you don't want us to hold your personal information this will restrict your ability to attend our classes and be a student of Goodwin Martial Arts.

Your additional individual rights

Where Goodwin Martial Arts holds personal information about you, you have a number of additional rights. These are quite straightforward.

The Right to be informed

That's what this notice does; it tells you what personal information we collect, what we do with it, who we share it with and how long we hold it for.

The right to access

This just means that you can ask us at any time to let you know what personal information we hold about you and we'll provide you with a copy.

If you want to know what personal information we hold about you, you can contact us at tamzingoodwin@sky.com and we'll provide you with the information. We have a month to get it to you but we'll try and make sure it's quicker than this.

You can ask us to provide your personal information in a form that is easily transferrable to another organisation and which can be extracted by software. This is called the right of data portability

The right to rectification

If we've got anything wrong this gives you the right to get us to correct it. We'll do this immediately. We try to ensure all your personal information is up to date.

When you are a member of Goodwin Martial Arts we ask you to let us know of any changes to your personal information. We do this explicitly when we ask you to renew your annual membership but you can do this at any time.

If you tell us we've got something wrong, and we've shared that with another organisation as described in the section called "Who we share your data with", we'll tell them the correct information to enable them to update their records.

The Right to Withdraw Consent

Each time we contact you before you become a student, we give you the right to "withdraw consent". This means you can tell us not to contact you again about our classes. If you do this we will delete your details.

Once you become a student we will only contact you with information about being a student with Goodwin Martial Arts. You do have the right to withdraw consent but this will only apply to direct marketing activity such as emails about the sale of t shirts and hoodies which are not required in order to train with Goodwin Martial Arts.

How to complain

Please let us know if you are unhappy with how we have used your personal information. You can contact us at tamzingoodwin@sky.com.

You also have the right to complain to the Information Commissioner's Office. Find out on their website https://ico.org.uk/concerns/

Other Websites

Our website contains links to other websites. This privacy policy only applies to Goodwin Martial Arts so when you link to other websites you should read their own privacy policies.

Changes to our Privacy Policy

We keep our privacy policy under regular review and we will place any updates on this web page. This privacy policy was updated on 25th May 2018

END

Appendix One - Checklist Commentary

The following is included to provide a quick validation for each item in our privacy policy based on the ICO checklist, and in some cases our rationale (where it is viewed as an area of complexity).

What to provide

We provide individuals with all the following privacy information:

☐ The name and contact details of our organisation.

Provided by the Goodwin Martial Arts privacy Notice

☐ The name and contact details of our representative (if applicable).

☐ The contact details of our data protection officer (if applicable).

Provided by the Goodwin Martial Arts privacy Notice, one person will act as both representative and DPO

☐ The purposes of the processing.

Provided by the Goodwin Martial Arts privacy Notice

☐ The lawful basis for the processing.

Provided by the Goodwin Martial Arts privacy Notice

☐ The legitimate interests for the processing (if applicable).

Not applicable to the Goodwin Martial Arts privacy Notice – we are not replying on legitimate interest.

☐ The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).

Not applicable to the Goodwin Martial Arts privacy Notice – however we have provided a list of personal data for transparency purposes.

☐ The recipients or categories of recipients of the personal data.

Provided by the Goodwin Martial Arts privacy Notice

☐ The details of transfers of the personal data to any third countries or international organisations (if applicable).

Provided by the Goodwin Martial Arts privacy Notice

☐ The retention periods for the personal data.

Provided by the Goodwin Martial Arts privacy Notice

☐ The rights available to individuals in respect of the processing.

Provided by the Goodwin Martial Arts privacy Notice

☐ The right to withdraw consent (if applicable).

Provided by the Goodwin Martial Arts privacy Notice

☐ The right to lodge a complaint with a supervisory authority.

Provided by the Goodwin Martial Arts privacy Notice

☐ The source of the personal data (if the personal data is not obtained from the individual it relates to).

We rely on the individual or a parent / guardian to provide us with the personal information – as such we don't feel that this is relevant (believe that the spirit of the regulation is in relation to sources a data subject may not be aware of)

☐ The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

Provided by the Goodwin Martial Arts privacy Notice

☐ The details of the existence of automated decision-making, including profiling (if applicable).

Not applicable to the Goodwin Martial Arts privacy Notice

When to provide it

☐ We provide individuals with privacy information at the time we collect their personal data from them.

Goodwin Martial Arts will provide:

- link to privacy policy from our "lead contact" form. Form will also explain that we will use their personal information to contact them about our classes.

- Privacy policy in full will be available to see on request and on our website.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

NOT APPLICABLE to Goodwin Martial Arts

☐ within a reasonable of period of obtaining the personal data and no later than one month;

☐ if we plan to communicate with the individual, at the latest, when the first communication takes place; or

☐ if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

☐ concise;

☐ transparent;

☐ intelligible;

☐ easily accessible; and

☐ uses clear and plain language.

Changes to the information

☐ We regularly review and, where necessary, update our privacy information.

☐ If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

☐ We undertake an information audit to find out what personal data we hold and what we do with it.

☐ We put ourselves in the position of the people we're collecting information about.

☐ We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

☐ a layered approach;

☐ dashboards;

☐ just-in-time notices;

☐ icons; and

☐ mobile and smart device functionalities.

Appendix Two – ICO Guidance (at a glance)

At a glance

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.

- You must provide privacy information to individuals at the time you collect their personal data from them.

- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.

- User testing is a good way to get feedback on how effective the delivery of your privacy information is.

- You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.

- Getting the right to be informed correct can help you to comply with other aspects of the GDPR and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

Checklists

What to provide

We provide individuals with all the following privacy information:

☐ The name and contact details of our organisation.

☐ The name and contact details of our representative (if applicable).

☐ The contact details of our data protection officer (if applicable).

☐ The purposes of the processing.

☐ The lawful basis for the processing.

☐ The legitimate interests for the processing (if applicable).

☐ The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).

☐ The recipients or categories of recipients of the personal data.

☐ The details of transfers of the personal data to any third countries or international organisations (if applicable).

☐ The retention periods for the personal data.

☐ The rights available to individuals in respect of the processing.

☐ The right to withdraw consent (if applicable).

☐ The right to lodge a complaint with a supervisory authority.

☐ The source of the personal data (if the personal data is not obtained from the individual it relates to).

☐ The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

☐ The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it

☐ We provide individuals with privacy information at the time we collect their personal data from them.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

☐ within a reasonable of period of obtaining the personal data and no later than one month;

☐ if we plan to communicate with the individual, at the latest, when the first communication takes place; or

☐ if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

☐ concise;

☐ transparent;

☐ intelligible;

☐ easily accessible; and

☐ uses clear and plain language.

Changes to the information

☐ We regularly review and, where necessary, update our privacy information.

☐ If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

☐ We undertake an information audit to find out what personal data we hold and what we do with it.

☐ We put ourselves in the position of the people we're collecting information about.

☐ We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

☐ a layered approach;

☐ dashboards;

☐ just-in-time notices;

☐ icons; and

☐ mobile and smart device functionalities.

What's new under the GDPR?

The GDPR is more specific about the information you need to provide to people about what you do with their personal data.

You must actively provide this information to individuals in a way that is easy to access, read and understand.

You should review your current approach for providing privacy information to check it meets the standards of the GDPR.

What is the right to be informed and why is it important?

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing people with clear and concise information about what you do with their personal data.

Articles 13 and 14 of the GDPR specify what individuals have the right to be informed about. We call this 'privacy information'.

Using an effective approach to provide people with privacy information can help you to comply with other aspects of the GDPR, foster trust with individuals and obtain more useful information from them.

Getting this wrong can leave you open to fines and lead to reputational damage.

What privacy information should we provide to individuals?

The table below summarises the information that you must provide. What you need to tell people differs slightly depending on whether you collect personal data from the individual it relates to or obtain it from another source.

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓

The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓

The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

When should we provide privacy information to individuals?

When you collect personal data from the individual it relates to, you must provide them with privacy information at the time you obtain their data.

When you obtain personal data from a source other than the individual it relates to, you need to provide the individual with privacy information:

- within a reasonable of period of obtaining the personal data and no later than one month;
- if the data is used to communicate with the individual, at the latest, when the first communication takes place; or
- if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

You must actively provide privacy information to individuals. You can meet this requirement by putting the information on your website, but you must make individuals aware of it and give them an easy way to access it.

When collecting personal data from individuals, you do not need to provide them with any information that they already have.

When obtaining personal data from other sources, you do not need to provide individuals with privacy information if:

- the individual already has the information;
- providing the information to the individual would be impossible;
- providing the information to the individual would involve a disproportionate effort;
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;

- you are required by law to obtain or disclose the personal data; or
- you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

How should we draft our privacy information?

An information audit or data mapping exercise can help you find out what personal data you hold and what you do with it.

You should think about the intended audience for your privacy information and put yourself in their position.

If you collect or obtain children's personal data, you must take particular care to ensure that the information you provide them with is appropriately written, using clear and plain language.

For all audiences, you must provide information to them in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

How should we provide privacy information to individuals?

There are a number of techniques you can use to provide people with privacy information. You can use:

- A layered approach – short notices containing key privacy information that have additional layers of more detailed information.
- Dashboards – preference management tools that inform people how their data is used and allow them to manage what happens with it.
- Just-in-time notices – relevant and focused privacy information delivered at the time individual pieces of information about people are collected.
- Icons – small, meaningful, symbols that indicate the existence of a particular type of data processing.
- Mobile and smart device functionalities – including pop-ups, voice alerts and mobile device gestures.

Consider the context in which you are collecting personal data. It is good practice to use the same medium you use to collect personal data to deliver privacy information.

Taking a blended approach, using more than one of these techniques, is often the most effective way to provide privacy information.

Should we test, review and update our privacy information?

It is good practice to carry out user testing on your draft privacy information to get feedback on how easy it is to access and understand.

After it is finalised, undertake regular reviews to check it remains accurate and up to date.

If you plan to use personal data for any new purposes, you must update your privacy information and proactively bring any changes to people's attention.

Appendix Three – Lawful Basis for Processing

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

How should we document our lawful basis?

The principle of accountability requires you to be able to demonstrate that you are complying with the GDPR, and have appropriate policies and processes. This means that you need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You need therefore to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. There is no standard form for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. This will help you comply with accountability obligations, and will also help you when writing your privacy notices.

It is your responsibility to ensure that you can demonstrate which lawful basis applies to the particular processing purpose.

What do we need to tell people?

You need to include information about your lawful basis (or bases, if more than one applies) in your privacy notice. Under the transparency provisions of the GDPR, the information you need to give people includes:

- your intended purposes for processing the personal data; and

- the lawful basis for the processing.

This applies whether you collect the personal data directly from the individual or you collect their data from another source.

What about special category data?

If you are processing special category data, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

What about criminal offence data?

If you are processing data about criminal convictions, criminal offences or related security measures, you need both a lawful basis for processing and a separate condition for processing this data in compliance with Article 10. You should document both your lawful basis for processing and your criminal offence data condition so that you can demonstrate compliance and accountability.

Contract as a legal Basis

At a glance

- You can rely on this lawful basis if you need to process someone's personal data:
- to fulfil your contractual obligations to them; or
- because they have asked you to do something before entering into a contract (eg provide a quote).
- The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

When is the lawful basis for contracts likely to apply?

You have a lawful basis for processing if:

- you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract.
- you haven't yet got a contract with the individual, but they have asked you to do something as a first step (eg provide a quote) and you need to process their personal data to do what they ask.

It does not apply if you need to process one person's details but the contract is with someone else.

Note that, in this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, you both intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value). However, this is not a full explanation of contract law, and if in doubt you should seek your own legal advice.

When is processing 'necessary' for a contract?

'Necessary' does not mean that the processing must be essential for the purposes of performing a contract or taking relevant pre-contractual steps. However, it must be a targeted and proportionate way of achieving that purpose. This lawful basis does not apply if there are other reasonable and less intrusive ways to meet your contractual obligations or take the steps requested.

The processing must be necessary to deliver your side of the contract with this particular person. If the processing is only necessary to maintain your business model more generally, this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests.

What else should we consider?

If the processing is necessary for a contract with the individual, processing is lawful on this basis and you do not need to get separate consent.

If processing of special category data is necessary for the contract, you also need to identify a separate condition for processing this data. Read our guidance on special category data for more information.

If the contract is with a child under 18, you need to consider whether they have the necessary competence to enter into a contract. If you have doubts about their competence, you may wish to consider an alternative basis such as legitimate interests, which can help you to demonstrate that the child's rights and interests are properly considered and protected. Read our guidance on children and the GDPR for more information.

If the processing is not necessary for the contract, you need to consider another lawful basis such as legitimate interests or consent. Note that if you want to rely on consent you will not generally be able to make the processing a condition of the contract. Read our guidance on consent for more information.

If you are processing on the basis of contract, the individual's right to object and right not to be subject to a decision based solely on automated processing will not apply. However, the individual will have a right to data portability. Read our guidance on individual rights for more information.

Remember to document your decision that processing is necessary for the contract, and include information about your purposes and lawful basis in your privacy notice.

Relying on Contractual necessity (from ICO)

Where you must process personal data in order to provide a product or perform a service that the individual is requesting.

Examples where contractual necessity legal basis may apply:

Purchase – "I want to buy this product"

Quote – "I request a price quote for this product"

Access – "I want trial access to this service/platform"

Help – "I need customer service / helpdesk support"

Event – “I want to register to attend this free event/webinar”

Publish – “I want you to publish and promote my article”

Info – “I want to subscribe to news / info / newsletters / alerts”

Press – “I request press credentials for a show”

Job – “I want to apply for this job”

Special Category data

At a glance

- Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.
- In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.
- There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Bill will introduce additional conditions and safeguards.
- You must determine your condition for processing special category data before you begin this processing under the GDPR, and you should document it.

What’s different about special category data?

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9.

This is because special category data is more sensitive, and so needs more protection. For example, information about an individual’s:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;

- sex life; or
- sexual orientation.

What are the conditions for processing special category data?

- The conditions are listed in Article 9(2) of the GDPR:
- (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- (e) processing relates to personal data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member

State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

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 personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.(This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).
- 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 consult with children as appropriate 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 in 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 marketing 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.

Privacy notices

☐ Our privacy notices are clear, and written 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.

☐ As a matter of good practice, if we are relying upon parental consent then we offer two different versions of our privacy notices; one aimed at the holder of parental responsibility and one aimed at the child.

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.