



## **General Processing**

### **What are the lawful bases for processing?**

The lawful bases for processing are set out in Article 6 of the General Data Processing Regulation (GDPR). At least one of these must apply whenever we process your 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 do we decide which lawful basis applies?**

This depends on our specific purposes and the context of the processing and which lawful basis best fits the circumstances. We identify and record our lawful basis at the start of any processing. In some cases we may identify more than one basis applies.

To identify the lawful basis we consider a variety of factors, including:

- What is our purpose – what we are trying to achieve?
- Can we reasonably achieve it in a different way?
- Do we have a choice over whether or not to process the data?

As we are a 'public authority', where we can demonstrate that the processing is to perform our tasks as set down in UK law, then we rely on the public task basis for our processing. We may also rely on consent or legitimate interests in some cases, depending on the nature of the processing and our relationship with you in some specific circumstances (e.g. provision of victim services).

Where we rely on consent or legitimate interest, we take into consideration the wider context including:

- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is our relationship with the individual?
- Are we in a position of power over them?
- What is the impact of the processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Are we able to stop the processing at any time on request?

We may use Legitimate interests as our lawful basis where we need to keep control over the processing and where we are take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them.

On the other hand, where we are giving individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), we will rely on your consent.

### **How do we document our lawful basis?**

The principle of accountability requires us to be able to demonstrate that we are complying with the GDPR, and have appropriate policies and processes. We keep a record of which basis we are relying on for each processing purpose, and a justification for why we believe it applies to help us comply with accountability obligations.

### **What about special category data?**

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection (Article 9(1) of the GDPR refers).

If we are processing special category data, we identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9 and document both our lawful basis for processing (Article 6) and our special category condition (Article 9) so that we can demonstrate compliance and accountability. These conditions do not have to be linked.

There are ten conditions for processing special category data in the GDPR itself (see Article 9(2) conditions below), as well as additional conditions and safeguards in the Data Protection Act 2018. We determine our condition for processing special category data before we begin this processing under the GDPR and document it.

### **Special category data – Article 9(1)**

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Paragraph 1 (above) shall not apply if one of the conditions listed in Article 9(2) applies.

## **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.

## **What about criminal offence data?**

When processing data about criminal convictions, criminal offences or related security measures, we identify and record both a lawful basis for processing and a separate condition for processing this data in compliance with Article 10 to demonstrate compliance and accountability.

## **What does Article 10 say?**

Article 10 says:

“Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”

## **Lawful bases – our criteria for using the below lawful bases:**

### **1. Consent**

The GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance our reputation.

When relying on consent we comply with the following:

- Consent requires a positive opt-in. We do not use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- We keep consent requests separate from other terms and conditions.
- Consent has to be specific and ‘granular’ (i.e. get separate consent for separate things. Vague or blanket consent is not enough).
- Be clear and concise.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how on the relevant form.
- We keep evidence of consent – who, when, how, and what we told you.
- We keep consent under review, and refresh it if anything changes.
- We will not make consent to processing a precondition of a service.
- We ensure the consent is freely given, and avoid over-reliance on consent where another lawful basis for processing is more relevant.

### **2. Contract**

We rely on this lawful basis if we need to process someone’s personal data:

- to fulfil our contractual obligations to them; or
- because you have asked us to do something before entering into a contract (e.g. provide a quote).

We will only rely on contract where the processing is necessary and we could not reasonably do what you want without processing your personal data.

### **3. Legal obligation**

We rely on this lawful basis if we need to process the personal data to comply with a common law or statutory obligation. We will identify the specific legal provision or an appropriate source of advice or guidance that sets out our obligation.

- This does not apply to contractual obligations.
- The processing must be necessary. If we can reasonably comply without processing the personal data, this basis does not apply.

### **4. Vital interests**

We rely on vital interests as our lawful basis if we need to process the personal data to save or protect someone's life.

- The processing must be necessary. If we can reasonably protect the person's vital interests in another, less intrusive way, this basis will not apply.
- We do not rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

### **5. Public task**

This lawful basis is relevant to us as we are a 'public authority'. We rely on this lawful basis if we need to process personal data:

- 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
- to perform a specific task in the public interest that is set out in law.

We do not need a specific statutory power to process personal data, but our underlying task, function or power must have a clear basis in law.

The processing must be necessary. We will not rely on public task basis if we can reasonably perform our tasks or exercise our powers in a less intrusive way.

Our considerations will include:

- Are we processing the data to carry out our official tasks or functions, or other specific tasks in the public interest?
- Can we point to a clear basis in law for your task or function?
- Is there another reasonable way to perform our tasks or functions without processing the data?

### **6. Legitimate interests**

We may rely on Legitimate interests in limited circumstances but, as a 'public authority', we will not often utilise this as a lawful basis for processing.

Legitimate interests are most appropriate where we use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

We can only rely on legitimate interests if we are processing for a legitimate reason other than performing our tasks as a public authority.

Where we rely on legitimate interest we will:

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

The legitimate interests can be our own interests or the interests of third parties and can include commercial interests, individual interests or broader societal benefits. The processing must be necessary and not reasonably achievable in another less intrusive way.