GDPR Grounds for Processing 1.0

Monday, 14 May 2018

Introduction

There are six lawful bases for processing data, and all of our processing activities must fit into one category or another. No one basis is better than another and several may apply depending on the category of data in question. The lawful basis should be established before the processing begins and it is important to get the basis correct the first time; the ICO states that you should not swap to another basis at a later time without good reason.

However, because of the slight shift in lawful bases that the introduction of GDPR is bringing, the ICO has confirmed that we may take this one off opportunity to re-assess their lawful bases and choose a new basis if the original one is no longer appropriate under GDPR.

If our purposes change or we identify a new purpose, we can keep the same lawful basis so long as the new purpose is compatible with the old purpose. To be compatible, it must not be very different from the original purpose, unexpected or have an unjustified impact on the data subject. In these cases, we would need to identify a new lawful basis. Changing purposes is dealt with differently when consent is the basis used. See "Obtaining consent" below for more on this.

Lawful basis for processing data

The lawful bases under GDPR are where:

- the data subject has given consent to the processing
- 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 the contract
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary in order to protect the vital interests of the data subject of another natural person
- processing is necessary for the performance of a task carried out in the public interest or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by 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.

Consent

Consent has been, until now, a frequently used lawful basis upon which organisations process their employees' data and essentially means that you have obtained confirmation from the data subject that you may process their personal data for your purposes. Many organisations inserted a clause

regarding the giving of consent into their employee handbook or other documentation and a signature to agree to all of the terms within the documentation assumed consent to data processing. Where electronic means were used, pre-checked tick boxes may have been used.

Under GDPR, the standard for obtaining consent is much higher and a clause within an employee handbook, for example, will not be sufficient. Consent must be freely given, obvious, unambiguous and explicit. It requires positive opt-in expressed in words rather than in the form of any other positive action. Requests for consent must be concise, easy to understand and in a standalone document setting out distinct processing purposes. Genuine consent puts the data subject in control; pre-ticked opt in boxes are not permitted.

The ICO states that **whilst obtaining consent is difficult, it may not be necessary** and you should assess whether another basis can be used. **If the nature of the data is such that you would process it regardless of a failure to receive consent, then consent is not an appropriate basis** and another should be sought. If you prefer to give individuals a real choice over whether their data will be processed or not then consent is likely to be an appropriate basis.

The higher standard required to use consent as a lawful basis creates difficulties for organisations. Under GDPR, consent will not be a lawful basis for processing where there is a clear imbalance of power between the data subject and the data controller. The ICO acknowledges, in its draft guidance on consent, that the employer-employee relationship is such that this imbalance is likely to exist. An individual may not feel like he/she has a choice over whether to give consent for fear that they may not be offered a job or may lose their job. For this reason, you should attempt to establish another lawful basis unless the employee has a genuine choice over whether to provide consent and no negative consequences would occur if consent was not given or withdrawn. For example, consent is likely to be the lawful basis in the situation when you decide to film within the office and you ask employees whether they would mind being in the background of the film. You should seek specific consent to this and if the employee refuses, you would simply need to ensure they were not in shot at any time.

Data subjects must be given the right to withdraw consent at any time after it has been given, therefore a consent request must inform data subjects of this right and how they may exercise it. If, the case of withdrawn consent, you would continue to process data, consent is not the appropriate basis.

A data subject's rights of erasure and portability apply to the basis of consent. Whilst the right to object does not apply, data subjects may withdraw consent at any time.

Obtaining consent

Where consent is the appropriate lawful basis, you should seek to obtain it in a freestanding, clearly set out document using easy to understand language. The request should include:

- the name of your organisations
- the name of any third party controllers who rely on the consent
- the reason for processing the data
- what the processing will involve
- the right of the data subject to withdraw consent.

Where different purposes of processing will take place, they can be covered in one document, however, you must set out each purpose clearly and allow positive opt in, or otherwise, for each.

Where your purposes for processing data for which consent was received change over time, you must obtain fresh consent to cover the new purpose or find another lawful basis.

You should make a record of the consent process. The duration of consent is not fixed. If the reason for processing changes, you should seek to review consent.

Performance of a contract

The operation of this lawful basis is almost identical to its operation under the Data Protection Act 1998. It applies when data processing is necessary in order to perform your side of the employment contract with the data subject eg to ensure that an employee is paid for their work you will need to process some of their personal details and their bank account details. This basis will apply to many elements of the employment relationship.

Where this is used as the lawful basis of processing data, you do not need to obtain the employee's consent.

A data subject's rights of erasure and portability apply to this lawful basis. The right to object does not apply.

Legal requirement

This basis is distinct from that which applies to contractual obligations and can be used when you must process data in accordance with a common law or statutory obligation. The basis does not require there to be a legal requirement for you to process data, rather a need to process data in order to meet a legal requirement. For example, you will need to process employee payroll data in order to ensure the correct payment of tax and National Insurance. You should be able to identify the obligation in question although this does not place an onus on you to find the relevant piece of law. Reference to a government website or other industry guidance explaining the general legal requirement will suffice.

Where you are processing data under the legal obligation basis, data subjects do not have the right of erasure, portability or the right to object.

Vital interests

This basis would apply when processing is necessary in order to protect someone's life. As such, it is not likely to be used in the employment context.

A data subject's right of erasure applies to this lawful basis. The rights to portability and objection do not apply.

Tasks in the public interest

This lawful basis would be used when it is necessary to process data in the exercising of an official authority, covering 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. This basis, although new, operates in a similar way to the old condition for "functions of a public nature". It is not exclusively for use by public authorities; it can be used by private sector organisations carrying out a task considered to be a function of public administration.

However, in reality, private sector organisations are likely to rely on the legitimate interests basis. Public authorities can no longer rely on the basis of legitimate interests for processing carried out in the performance of their public tasks. The "public interest" task should be considered instead.

A data subject's right of erasure and portability do not apply to this lawful basis. However, the right to object does apply.

Legitimate interests

This lawful basis has the widest scope and may be used for purposes which are not required by either the law or the employment contract. Legitimate interests may include the ability to defend itself against claims in the Employment Tribunal by keeping data of unsuccessful job applications for some time after rejection. The legitimate interests may be yours or of third parties, commercial interests or societal interests.

Using this basis brings extra obligations on organisations. You must ensure that people's rights and interests are fully considered and protected. If the processing activity would create an imbalance between the interests of the employer and the rights of the employee, it will not be appropriate to use this basis. ICO guidance states that is it most likely to be used when you process data in ways that people would reasonably expect and that have minimal privacy impact. It discourages use where:

- you are using data in ways people would not reasonably expect
- you are using data in ways people would not understand
- you think some people would object if you explained it to them
- the processing could cause harm unless you are confident there is a compelling reason to go ahead which justifies the impact.

Public authorities may rely on this basis for processing data which is not done in the performance of their public task eg processing employee data in the capacity of the employer. For data processed in the performance of their public tasks, the public authority should consider using the public interest basis.

Because the legal requirement and performance of a contract basis are more clear cut, you may find yourself in a position to decide whether the basis of consent or legitimate interest is the appropriate basis. Because using consent gives data subjects the control over how their data is used and allows them to withdraw consent at any time, the basis of legitimate interests is likely to be more appropriate if you prefer to keep control over the process, while demonstrating that it is line with people's expectations and would not have an unwarranted impact on them.

A data subject's right of erasure and right to object apply to this lawful basis. The rights to portability does not apply.

Three step test for using legitimate interest basis

To assess whether the legitimate interest basis applies, the ICO recommends you use a three step test:

Are you pursuing a legitimate interest?

- Why do you want to process the data?
- Who benefits from it and how?
- How important are the benefits?

- What would be the impact if you could not go ahead with the processing?
- Would your use of the data be unlawful or unethical?

Is the processing necessary for that purpose?

- Does the processing help to further that interest?
- Is it a reasonable method to adopt?
- Is there another less intrusive way to achieve the same result?

Consider the impact of the processing and whether this overrides the interest you have identified

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on them, and how big might the impact be?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt out?

You should record your decision making and keep it under review in case there is a change in the purpose for the processing. You must be confident that your legitimate interests are not overridden by the risks you have identified and if you have any doubts, a different lawful basis may be more appropriate.

Lawful basis for processing data

Additional obligations apply when special category data is processed.

Special category data is data that relates to a data subject's:

- race
- ethnic origin
- political opinion
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation.

Where data falling into the categories above are used, you must identify a lawful basis from the six detailed above as well as an additional basis from those specific to the special category condition. These are:

- the data subject has given explicit consent to the processing
- processing is necessary for carrying out obligations and rights of the controller or of the data subject in the field of employment law, and other laws, so far as it is authorised by law
- processing is necessary to protect the data subject's vital interests
- processing is carried out, in the course of its legitimate activities, by a body with a political, philosophical, religious or trade union aim
- processing relates to personal data which are manifestly made public by the data subject

- processing is necessary for the establishment, exercise or defence of legal claims
- processing is necessary for reasons of substantial public interest
- processing is necessary for the purposes of preventative or occupational medicine and for other medical purposes
- processing is necessary for reasons of public interest in the area of public health
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes

Criminal offence data

As with special category data, additional obligations apply.

You may only process criminal offence data where you have a lawful basis and are either processing the data in an official capacity or have specific legal authorisation.

The Data Protection Bill will set out more information on this but it is likely to state that criminal offence data may be processed where it is necessary under employment law where there is an appropriate policy in place.

Deciding on a lawful basis

You will need to establish the lawful basis for processing data before you start processing it.

You should first consider why you are processing the data. In certain cases, the basis will be obvious, for example, when the purpose of processing is so that you may comply with a legal requirement, or in line with a contractual obligation.

You may find it useful to begin with an initial consideration of whether the legal obligation or the performance of a contract bases apply and if not, then go on to consider the others. Note that not all bases will be an option depending on, for example, whether you are a public authority.

Where the processing is not done on the basis of legal requirement or the performance of a contract, the decision over which basis applies may be more difficult.

Where no lawful bases apply, you should stop processing the data.

Documenting your lawful basis

You should keep a record of the lawful basis which applies to each type of processing in order to demonstrate that you are complying with GDPR and in line with the accountability principle.

Where consent is the lawful basis, you will need to keep additional records illustrating that consent has been obtained from the data subject.

Where the legitimate interest basis is used, you must let data subjects know of the legitimate interest in your privacy notice.

QUINTADENA POLICY.

So far as the processing of customer / supplier / prospect data is concerned, the ground will be **LEGITIMATE INTEREST** up and until the point where an order is placed or received, whereafter it will be both **LEGITIMATE INTEREST** and **PERFORMANCE OF A CONTRACT**.

So far as the (potentially) sensitive personal data we hold regarding our Directors and Staff is concerned, **LEGITIMATE INTEREST** will be supplemented by **CONSENT** and / or the processing being **necessary under employment law**.

MOC
Thursday, May 17, 2018