When is processing personal data in your legitimate interests?

INTRODUCTION

Under EU legislation, the processing of personal data has to be fair and lawful, which requires, among other things, that one of six specified legal grounds applies. Much of the processing of personal data that takes place today in the EU, and particularly in the UK, relies on the ‘legitimate interests’ ground, as set out in Article 7(f) of Directive 95/46/EC (the ‘Directive’).

The Article 29 Data Protection Working Party (the ‘WP’) has identified that there is a lack of harmonisation of the interpretation of the legitimate interests ground which has led to divergent applications across the EU. The WP are concerned that this has created a lack of legal certainty and predictability over the years and may have imposed unnecessary regulatory burdens on organisations, especially those operating cross-border. The WP have therefore released their opinion on the notion of legitimate interests of the data controller (the ‘Opinion’). Opinions from the WP are not legally binding, but they are always useful in showing how regulators across the EU may approach an issue.

Interestingly, the WP also took the opportunity to discuss each of the six legal grounds, not just the legitimate interests ground, and provides examples of how they would (and would not) apply in various scenarios. The Opinion is therefore a useful reference whichever of the legal grounds is under consideration.

WHAT IS THE LEGITIMATE INTERESTS GROUND?

The processing of personal data will be fair and lawful where it is necessary for the legitimate interests of an organisation (the data controller) or of any third party to whom the data are disclosed, provided that those interests are not overridden by the interests or fundamental rights of the individuals whose data are being processed.

The WP suggest that when assessing whether the legitimate interests ground can be relied, the analysis should reflect the following steps:

1. Determine if an interest is legitimate or illegitimate
2. Determine whether the processing is necessary to achieve the interest pursued
3. Establish a provisional balance by assessing whether the data controller’s interest is overridden by the fundamental rights or interests of the data subjects

---

1 See also paragraph 6 of Schedule 2 of the Data Protection Act 1998 which implements Article 7(f) in the UK.
2 The WP is an independent European advisory body on data protection and privacy made up of representatives from the data protection authority of each EU Member State.
4. Establish a final balance by taking into account additional safeguards

5. Demonstrate compliance and ensure transparency.

**IS THE INTEREST LEGITIMATE?**

The WP accept that the notion of legitimate can include a broad range of interests, whether trivial or very compelling, simple or more controversial. In summary, the Opinion provides that to be legitimate, the interest must (i) be lawful, that is in compliance with relevant laws; (ii) be sufficiently clearly articulated so as to allow the balancing test to be carried out; and (iii) represent a real and present interest, that is it should not merely be speculative.

The Opinion lists various examples of situations where controllers may have a legitimate interest. This includes employee monitoring for safety or management purposes, IT and network security and conventional direct marketing and other forms of marketing or advertisement.

It also gives examples where the recipient of the personal data may have a legitimate interest in receiving it. The examples largely cover the benefit of public disclosure to, for instance, journalists, employees and the general public.

**IS THE PROCESSING NECESSARY?**

The processing must be necessary for the purpose of the legitimate interests pursued. It must therefore be considered whether other less invasive methods are available to achieve the legitimate interest. The necessity requirement applies to all the legal grounds for processing (other than consent), but the WP consider it to be particularly relevant in the context of the legitimate interest ground so as to prevent overly broad reliance on this ground.

**ESTABLISHING THE PROVISIONAL BALANCE**

The Opinion explains that the legitimate interests of the controller and the impact on the interests of the individuals can be seen on a spectrum. The WP are therefore of the view that important and compelling legitimate interests could justify significant intrusion in privacy or other significant impact on individuals’ interests, in a way that a minor legitimate interest would not.

The balancing exercise is a complex assessment which must be applied to the specific facts of the case rather than in an abstract manner. The Opinion sets out a number of factors for consideration.

**The impact on the data subject**

The Opinion clarifies that the relevant individuals are entitled to have all categories of interest taken into account, and not simply those that would be considered to be legitimate. In this regard the WP note that individuals engaged in illegal activity should also not be subject to a disproportionate interference with their rights and interests. Whilst this seems controversial on the first reading, presumably having identified such interests the nature of the interest can then be taken into account. The Opinion does not however state this.
In any event, the UK appears to have taken a slightly different approach. In the Data Protection Act 1998 (the ‘DPA’), the necessary legitimate interests of the controller (or third party recipient) will prevail except where the processing is unwarranted by reason of prejudice to the rights and freedoms and legitimate interests of the individual. This means that where an individual’s interests would usually prevail but the processing in question is ‘warranted’, the controller will be able to rely on the legitimate interests ground. For example, if a finance company passes the details of an indebted customer to a debt collection company, that disclosure would be warranted.

The way the data are processed

The volume of data being processed and how widely they are to be made accessible needs to be considered. The WP highlight that privacy impact assessments are a useful tool that can help in this regard.

Reasonable expectations of the individual

The reasonable expectation of the individuals with regard to the use and disclosure of the data are identified by the Opinion as being very relevant. It will be necessary to look at the specific facts of any situation as certain factors could give rise to reasonable expectations of stricter confidentiality or restricted use. Such factors would include the status of the controller, the nature of the relationship or service provided, the applicable legal or contractual obligations and any other promises made at the time of data collection.

Status of the data controller and the individual

Any imbalance in the relationship between the controller and the individual should be taken into account, including if the individual is an employee or student or if he is generally more vulnerable (e.g. a child). The status of the data controller is also relevant. For example, a data controller in a dominant position (whether because it is a large multinational, a public body or because it has a monopoly over a particular market) is likely to find it easier to ‘impose’ on the individual a course of action that is in the controller’s legitimate interests. Here, the Opinion echoes a preliminary opinion of the European Data Protection Supervisor dated March 2014 which suggested a wider role for data protection in ensuring that such dominance is not misused.

ESTABLISHING A FINAL BALANCE

The WP envisage that, if after establishing a provisional balance the answer is not clear cut, one can go on to consider how introducing additional safeguards could prevent undue impact on the relevant individuals in order to help tip the balance in favour of the controller.

Such additional safeguards could include strict limitations on the collection of data, functional separation of data so that it cannot be used to take decisions or other actions with respect to individuals, increased security measures, shorter retention periods, increased transparency and general and unconditional rights of the data subject to opt-out of the processing.

DEMONSTRATE COMPLIANCE AND ENSURE TRANSPARENCY

The Opinion suggests that it would be good practice to document the balancing exercise in a sufficiently detailed way so that, if necessary, this can be assessed by regulators in the future.

The WP also recommend that data controllers explain to individuals why they believe their interests prevail and what additional safeguards will be implemented to protect the individual’s interest, including the right to opt out.

---

3 This example is taken from the Information Commissioner’s Guide to Data Protection.
4 See our Client Briefing (March 2014).
Whilst under the DPA there is an obligation to provide fair processing information to individuals, the provision of this information would be a departure from practice in the UK.

This is simply a recommendation at present but the WP go on to suggest that its recommendations on the how to carry out the assessment, including the enhanced accountability and transparency obligations above, be included in the EU reform proposals as non-exhaustive factors to consider. If adopted, this would add to the administrative burdens that many organisations will already face if and when the reform goes ahead.

THE OTHER LEGAL GROUNDS

The Opinion also provides a useful analysis of the other five legal grounds for the processing of personal data. The analysis is illustrated with practical examples to help demonstrate where reliance on the legitimate interests would (or would not be) more appropriate.

Consent
The WP re-iterate their view that consent must be unambiguous and that this requires the use of mechanisms that leave no doubt of the individual’s intention. The Opinion specifically identifies that the use of default options that the user has to modify in order to object or reject the processing does not amount to unambiguous consent.

Performance of a contract
This ground applies where processing is necessary for the performance of a contract with the individual. The Opinion identifies various processing activities which would fall within this condition, such as processing address details to deliver goods or processing bank and salary information to pay employees. It also lists a number of situations which go beyond what is ‘necessary’ for the performance of the relevant contract and would therefore not satisfy this condition, including: monitoring employee communications and carrying out credit checks prior to the grant of a loan. The Opinion instead suggests that such activities should be subject to additional safeguards (as mentioned above) so that the legitimate interests ground can be relied upon. Obtaining consent would be another option.

Legal Obligation
The Opinion provides that controllers can rely on this ground when the processing is necessary to comply with a clear and specific legal obligation under the laws of the EU or a Member State. In the UK, this condition is interpreted as only applying to UK legal obligations such that compliance with the laws of another EU member state could not satisfy this condition. It is not clear from the Opinion if it is attempting to address this distinction.

A legal obligation imposed by non-EU countries will only therefore fall within this condition if it is integrated into national law, for example under an international agreement and, on the basis of the UK interpretation, this would also be the case for legal obligations under the laws of other EU member states. Usefully, however, the WP acknowledge that compliance with a foreign legal obligation may represent a legitimate interest of the controller.

Vital interests
The WP confirm that this ground applies where the processing of the data is necessary to protect the vital interests of an individual, effectively matters of life or death. The WP are of the view that a restrictive interpretation must be given to this provision such that it should not, for instance, be used to collect airline passenger data as a preventative measure against terrorism. It cannot therefore normally be used to legitimise any massive collection or processing of personal data.
Public task
In the Directive, this ground legitimises processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party recipient. The WP envisage that this could apply where a public authority competent for investigating crime requests a controller’s cooperation or where the controller discloses information voluntarily to such authority. In the UK, such situations are unlikely to be legitimised under the similar ‘public functions’ ground, which is much narrower than in the Directive.

Helpfully, however, the Opinion clarifies that, for now at least, public authorities can rely on the legitimate interest ground. Looking forward, the EU reform proposals appear to prevent this, which means that reliance on the public task ground by public authorities would increase.

COMMENT

The sixty-page long Opinion produced by the WP contains many useful practical examples and in-depth guidance to help data controllers, especially those trying to establish a common approach for processing activities across the EU. That said, as noted above, the DPA does not exactly track the wording of the Directive and so the relevant legislation in each member state must still be considered.

There will likely be situations where the balance of interests drawn up by the WP does not reflect the current and future plans of certain controllers. This is particularly so in relation to profiling and the combining of personal data across online services, where the WP believe the interests of individuals would generally prevail. However, organisations that implement the Opinion’s guidance on when to rely on the legitimate interests ground and how to apply the balancing test are likely to be in a very good position to demonstrate compliance with current best practice and to future-proof their processing activities.

*Paragraph 5, Schedule 2 of the DPA.*