Legitimate interests is not a new processing basis under the General Data Protection Regulation (‘GDPR’), and is probably the basis upon which most processing was performed under the previous law.

According to this ground for personal data processing (which appears in Article 6(1)(f) of the GDPR), a controller may process personal data where: ‘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.’

Whilst in the past, many controllers treated legitimate interests as a default or catch all position — many without even considering the rights of individuals — the GDPR has increased the focus on the balancing exercise involved. Legitimate interests will only justify processing where the ‘legitimate interests’ (of the controller, third parties and society at large) on one side outweigh the rights of the individual on the other side (broadly speaking). While not an explicit requirement under the GDPR, Supervisory Authorities have encouraged the drawing up of ‘legitimate interests assessments’ to document the assessment of whether the balancing exercise can be resolved in favour of the data processing.

Before looking at how to conduct the balancing exercise, it is worth noting that the choice of legitimate interests, as opposed to a different lawful basis, can be significant. For example, the legal rights available to individuals under the GDPR depend on the basis on which their data are being processed; a right to ‘data portability’ exists in relation to processing based on consent, but not that based on legitimate interests. This can be significant.

In some respects, consent and legitimate interests look very similar, with only the ‘default’ position being different. When consent is relied on, the processing may not be performed unless the individual consents (i.e. the default is no processing). When legitimate interests is relied on, the processing may be performed until (potentially) an individual objects (i.e. the default allows processing). Consent (which is of course also revocable) and legitimate interests (which implies an opt-out) start to look entirely symmetrical. However, they are not. When processing is based on consent, if an individual revokes his or her consent, such processing must stop. When processing is based on legitimate interests and somebody objects, the controller still has the opportunity to demonstrate that its compelling legitimate grounds prevail over the rights and interests of the individual, in which case the processing may continue.

What is legitimate?

Legitimate interests are very broad and, arguably, include anything that is not prohibited by European Union or Member State law. However, the ‘interest’ must be real and current; that is, it should be an interest that is being pursued now or in the near future, as opposed to some vague future aspiration. It should also be clear and articulated with a reasonable level of specificity; it is not sufficient for an interest simply to be ‘to make a profit’.

Recital 47 – 49 of the GDPR includes specific examples of processing that may be based upon legitimate interests, including fraud prevention, corporate administration within a group of companies, network security and direct marketing. Although the reference to direct marketing as a specific example of a legitimate interest is helpful, it is still necessary to perform the balancing exercise overall. The GDPR is not saying that direct marketing invariably prevails when the balancing exercise is carried out — far from it.

Once a legitimate interest has been identified, the processing based on it must also be considered ‘necessary’. This is best understood through the controller asking: ‘do I need to do this processing in order to fulfil the legitimate interest, or can the legitimate interest be fulfilled without some or all of the proposed data processing?’ Clearly, this overlaps with the concept of ‘proportionality’.

In this second of this two part series, Mark Watts, Partner at Bristows, looks at the key elements of legitimate interests as a grounds for data processing, before providing three case studies illustrating the applicability of consent versus legitimate interests. (For the first part, on consent, see Volume 19, Issue 2)
**Interests, rights and freedoms**

Just as legitimate interests are broad, so too are the interests, fundamental rights and freedoms of individuals on the other side of the balancing exercise. They are not limited to privacy rights, but other rights individuals may have must be taken into account too.

**The balancing exercise**

When undertaking the balancing exercise — that is, deciding whether the legitimate interests or individual rights prevail — a controller must, as required by Recital 47 of the GDPR, take into account the reasonable expectations of the individuals concerned. For example, would the individual expect the processing to occur?

This is where a data protection notice can be particularly effective during data collection. Such notices can be an opportunity for the controller to bring things to the attention of the individual so that they are within his or her reasonable expectation.

It is also necessary to consider the relationship between the controller and the individual concerned. For example, where the relation is a close one, such as where the individual is either an employee or a customer, it is more likely that the balancing exercise may be resolved in favour of the controller’s legitimate interests.

Another factor to take into consideration is the impact of the processing on the individual. This involves looking at both positive and negative impacts (though negative impacts should likely be given more weight), as well as the likelihood of such an impact and its potential severity. Finally, Article 6(1)(f) is clear that where the individuals concerned are children, far greater weight must be given to their various rights and freedoms.

Having conducted an initial assessment, a controller should consider what further safeguards might be brought to bear, to protect the individuals concerned. These may include data minimisation, the de-identification of the data concerned, other technical measures, including aspects of Privacy by Design, greater transparency (i.e. a clearer and more explicit notice), the availability of a means of opt-out and also the retention period for the data being processed. Overall, the greater and more effective the safeguards, the more likely it is that the ‘scales’ will tip in favour of the controller’s legitimate interests.

The following, real life-based scenarios demonstrate the applicability of consent versus legitimate interests.

**Case Study 1 – Employee Promotional Video**

A company is preparing a series of promotional videos for its website and for client presentations. The videos include interviews with selected staff members, footage of people eating lunch in the staff cafeteria and footage from client evening social events.

The company has engaged a production company to film and edit the footage, and may wish to continue to use it for up to three years.

Can consent be used as a lawful basis? Possibly, but it is likely to be difficult. The employer-employee relationship is often cited as a paradigm example of a relationship where there is an imbalance of power, and thus, it may be difficult to overcome the perception of ‘pressure’ by making it truly voluntary, with no downside to refusing consent.

There is, however, a greater downside. In order to be valid, any consent needs to be capable of withdrawal and any processing based on consent would need to stop from the moment of its withdrawal; it is not straightforward to ‘switch’ to another lawful basis and continue processing after consent has been revoked. This would present difficulties in respect of video content intended to be used for three years.

Interestingly, one often sees consent statements used in these situations, but typically they form part of a ‘release form’ that deals with other legal matters, such as intellectual property, image rights, passing off, etc. Historically, these release forms have tended to bundle in a data protection consent too, though since the GDPR, they tend to refer to legitimate interests as the more appropriate basis.

In terms of legitimate interests: there can be little doubt that making a promotional video, using it in presentations and having it on the company’s website, are legitimate. Does the processing necessity also need to be considered?

In all likelihood the answer is yes. To the extent that the promotional videos are intended to communicate the ‘feel’ of a company’s culture and its people, it’s hard to see how this may be done without featuring actual employees. It may be possible to raise a query perhaps about the use of social footage — is this really necessary?

Again, this will depend on the nature of the video intended, and perhaps
the nature of the company and its business. While concerns may be raised in relation to posting video footage of social events on the company’s website, these are better considered when weighing the balancing exercise.

What about the individuals’ (employees’) rights? The company should consider each individual’s right to privacy generally, as well as any potential impact on a specific individual. Context is very important here, as is whether the video is merely used ‘one on one’ in a client presentation, or is widely available via the company’s website, where everyone – friends, spouses, violent ex-spouses, etc. may see it. It might be embarrassing (or worse) for some individuals to be captured in a social situation, drinking perhaps, when their religion does not permit it.

What safeguards can be applied to ensure that the balancing exercise tips in favour of legitimate interests?

A very clear notice should be provided, describing the project, the areas where filming will take place, the time when it will take place, and so on. It should be possible for someone not to participate — attendance at the social event should be voluntary. Depending on the nature of the footage, it may be a good idea to show the content to the individuals involved, unless they only feature in the background in a way that they are unlikely to be recognised, and with no consequences even if they are. For videos where the content is more ‘personal’ in nature, it may even be necessary to allow individuals to influence the content through the editing process.

It should also be kept in mind that even where processing is based on legitimate interests, an individual still has the option to ‘opt out’ under Article 21 of the GDPR (closely related to his or her right of erasure under Article 17). In this situation, if an individual were to exercise this right, the company would need to cease processing unless it is able to demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the individual.

Whether the company is able to do so will be very context specific, and will depend on the details of the individual’s specific situation.

Case Study 2 – Automated Recruitment

A company is going through a recruitment process for a number of roles, and needs to sift through hundreds of applications. It wants to use a first stage online written test in which candidates are asked to respond to certain scenarios. A piece of software analyses candidate responses for inclusion of certain correct terminology, and awards them a score. Candidates with a score above a set amount progress to stage 1 interview.

This is an increasingly popular approach to recruitment. The facts as presented are not sufficiently clear to determine whether or not the initial ‘sifting’ should be considered an ‘automated decision’ under Article 22 of the GDPR. If it is, which would arise from there being no human involvement in the process of rejecting applicants, each applicant’s explicit consent will be required. This is particularly likely in the United Kingdom as a result of Article 22 of the GDPR being mistakenly interpreted not as a ‘right that needs to be exercised’, but rather as a ‘general prohibition’ in Section 49 of the Data Protection Act 2018.

If explicit consent is required, the issue that arises is whether seeking such consent in the context of recruitment can ever be considered ‘freely-given’. While there is no employer-employee relationship at this stage, nor can it be said that refusing consent is without detriment, unless the company provides an alternative route for stage 1 of their process that does not involve an automated decision (i.e. with human involvement). This, of course, would undermine many of the efficiency gains it hopes to achieve, as well creating a risk of (say) discrimination, bias or some other form of unfairness as a result of human involvement.

Of course, a similar argument can be levelled at consent in the context of ‘ordinary’ recruitment; that is, recruitment without any automated decision making, having human involvement at each stage in the process. Can consent work in circumstances where the only alternative for the applicant is not to apply? It seems unlikely, and the detriment too great.

In practice, however, one might reasonably assume that applicants keen to get a particular job are unlikely to object to the proposed processing of their data (CV, etc.) unless their consent is being for processing that is wholly necessary or unreasonable. Nevertheless, consent presents a challenge to recruitment, and, increasingly, data processing as part of a recruitment process is being based on Article 6(1)(b) — that the ‘processing is necessary… in order to take steps at the request of the [individual] prior to entering into a contract’, although this lawful basis is not the subject of this article.

Putting aside the possibility of the CV sifting here being an automated decision that requires explicit consent, it is worth considering whether legitimate interests may be relied upon. Recruitment is clearly a legitimate interest, as are the goals of increasing efficiency in the recruitment process, reducing cost and potentially reducing the effects of unconscious bias through partly automated tools. Moreover, provided that the personal data processed is within the bounds of typical recruitment, the processing of their CV can also be considered as necessary.

What of the applicant’s interests, fundamental rights and freedoms?

There are potentially many, for example, the ‘right’ to have one’s application considered properly and fairly, with appropriate weight attached to factors such as actual experience as opposed to academic qualifications, the ‘right’ not to be treated as just a ‘number’, and so on. And applying the balancing exercise, taking into account that there is not a close relationship between the company and the applicant, that there may be a significant negative impact on the individual through a ‘bad’ decision, an initial assessment may resolve it in favour of the applicants’ rights.

However, there are many safeguards
that can be applied to tip things the other way. A clear notice that describes the processing can be provided. More human involvement may be brought to bear. A better, more thoroughly tested algorithm may be used. The automated sifting component may be used more sparingly, perhaps only to identify the applicants that are wholly unsuitable. An appeal process involving human review may be offered to applicants, even though it is not strictly required under the GDPR for decisions not caught by Article 22.

Case Study 3 – The Smart Watch

A company is launching a smart watch product, which monitors heart rate, sleep time, and maps workout routes and distance travelled. Users can use a linked app to see their workout results, track their progress and compare their stats to other users through a workout leader board. They can also upload photos of them using the watch, and provide written comments and feedback, which the company may use on its website and promotional materials.

The company also uses the device data to analyse commonly used workout times and distances in order to improve how it presents information on the App, and to check that the devices are working as intended.

In cases such as these, a considerable amount of personal data are likely to be processed, including photographs, health data and geolocation data. In respect of both health data and geolocation data, there is no realistic alternative to consent (explicit consent in the case of health data).

The Smart Watch also processes data for a variety of different purposes – basic watch functions, sharing workout stats, photo sharing, promotional purposes and product improvement. As a result, any consent that is to be relied upon needs to be both sufficiently informed (the device’s technical complexity explained in plain, accessible language) and specific (the various different purposes need to be individually identified). On top of this, any consents need to be granular, so a simple, ‘I consent to everything’ approach will not work.

Equally, while much of the processing may be considered as ‘necessary’ for the performance of the Smart Watch (and accompanying service), much of it – the promotional use and the product development in particular – is not, and so any attempt to ‘condition’ or ‘tie’ consent to the processing necessary to perform the functions for which the device was bought, is unlikely to be valid.

As well as there needing to be separate consents, these consents need to be capable of being easily revoked. Typically, in these devices (and/or any accompanying mobile app or dashboard), revocation is offered via a device setting, such as ‘location ON/OFF’. To the extent that consent is being relied upon, it needs to be indicated by an affirmative act (and an affirmative statement in the case of special category data). This is usually obtained as part of the initial device set up process, with the possibility to consent to more or less through the device thereafter.

For some of the purposes described, legitimate interests is likely to be a better lawful basis. For example, product improvement is clearly legitimate and the ‘necessity test’ is likely to be met, especially if the personal data involved are minimised. Ideally, an anonymous or at least pseudonymous data set should be used for product improvement purposes. Where this is the case, there should be little or no impact on any individual, so that legitimate interests may be relied upon. Other additional safeguards, such as minimising the data retention period, may also be implemented.

As for the ‘regular’ Smart Watch functions, it is likely that the majority of the processing these involve may be based on either Article 6(1)(b) (‘contractual necessity’) or Article 6(1)(f) (‘legitimate interests’).

Conclusion

No one lawful basis is always better than the other. Far from consent always being the best, it is often the least appropriate and the most difficult to use, particularly having regard to the requirement that it can be easily withdrawn.

Equally, while under the previous law, legitimate interests was the ‘default’ or ‘catch all’ processing basis for a lot of processing, this is less obviously now the case, with a much greater focus on the need to conduct a balancing exercise. Controllers need to think carefully about the most appropriate lawful basis for each aspect of their processing.

Mark Watts is leading a Workshop on ‘consent’ at the 18th Annual Data Protection Compliance Conference, taking place in London on 10th and 11th October 2019. For further information, see www.pdpconferences.com

Mark Watts
Bristows
mark.watts@Bristows.com