Processing of personal data: consent and legitimate interests under the GDPR

The General Data Protection Regulation (GDPR) introduces a wide range of reforms to the European data protection regime which will continue to be relevant for many companies regardless of the UK's future relationship with the EU. The GDPR introduces a number of changes to the concept of "consent" as a condition to lawful processing, as well as updating and revising the general principles of processing and the "legitimate interests" condition. Many of these changes formalise current best practice and this briefing explores what has changed and the implications for those who rely on these conditions to operate their business.

Grounds for lawful processing under the GDPR

As is the case under the Data Protection Act (DPA), the processing of personal data must fall within one of six specified conditions. The differences in the commonly used "consent" and "legitimate purpose" conditions under the GDPR are shown below.

	DPA	GDPR
Consent Condition	The data subject has given his consent to the processing	The individual has given consent to the processing of his or her personal data **for one or more specific purposes**
Legitimate Purpose Condition	The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is **unwarranted** in any particular case by reason of prejudice to the rights and freedoms or **legitimate interests** of the data subject	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. This shall not apply to processing carried out by public authorities in the performance of their tasks**

Meaning of consent

The concept of consent in the GDPR is stricter than in the DPA, setting out more onerous requirements in relation to both the content of consent and the way in which it should be obtained.

Where processing is based on consent, companies must be able to demonstrate that consent was given by the individual to the processing of the personal data. The GDPR defines consent as:

> any **freely given, specific, informed and unambiguous** indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.
>
> (Emphasis added)

Taking each of these concepts in turn:

Consent must be freely given

As currently, individuals should have a genuine and free choice as to whether or not to consent to the processing and should be able to refuse or withdraw such consent without detriment. However, the GDPR provides that consent will **not** be "freely given" where the performance of a contract, including the provision of a service, is conditional on consent to the processing of data that is not necessary for the performance of the relevant contract.

This raises a question over the legitimacy of the many "free" digital services which are offered on the condition that users agree to receive marketing information. A strict reading of the GDPR suggests that individuals' consent cannot be relied upon in these circumstances because the details are not necessary for the performance of the service and, therefore, the consent is not freely given.

The Article 29 Working Party's (A29WP) previous guidance on consent under the Data Protection Directive (Directive) supports this interpretation. In that guidance, the A29WP considers whether a social network service could require users to consent to certain processing as a condition to providing the service. The A29WP concluded that users should be put in a position to give free and specific consent to any processing which goes beyond what is necessary to deliver the service.

Freely given consent in an employment context

The extent to which consent can be relied upon in the employment context to justify the processing of personal data is already doubtful under the DPA regime, as reflected in both the ICO's and the A29WP's guidance. Unsurprisingly, this position will remain the same under the GDPR: it is clear that consent will not be an appropriate ground where there is a "clear imbalance between the data subject and the controller". This will not always be the case in an employment context (see the "intranet" example below) but, in general, processing by employers will need to be carried out under a different ground.

A similar point is made by the A29WP in its July 2016 opinion on the ePrivacy Directive, which considers how the directive should be revised to ensure it is future proof.

Consent must be specific and informed

These requirements were present in the EU Data Protective Directive (Directive), which the DPA implements. However, the GDPR clarifies that consent can only be informed if the individual is aware at least of the identity of the company which is the "data controller" and the purposes of the processing of his or her personal data. If the intended processing covers multiple purposes, consent must be granted for all such purposes.

There should, therefore, be a specific choice as to which purpose the individual consents to, rather than there being an all-inclusive consent to data processing for multiple purposes.

Consent in a written declaration

Unlike currently, the GDPR requires that where consent is given as part of a written declaration which also concerns other matters, the request for consent should be "clearly distinguishable" from the other matters and be presented in an "intelligible and easily accessible form". It will be important, therefore, to ensure that a data subject's consent to processing is not buried in standard terms and conditions but is instead set out separately from other provisions.

Whilst the objective of "unbundling" is to provide individuals with greater control over their data, there is a potential tension with the requirements that information and communications relating to processing be easily accessible and easy to understand. Companies which rely on consent for multiple processing purposes will likely wish to adopt a cautious approach to the specific consent requirements, but communicating this to individuals in a way they can understand may not be a straightforward task.

Consent must be unambiguous

Under the GDPR, consent must be "unambiguous", a concept which existed in the Directive but was not used in the DPA. The GDPR also requires the consent to be explicit in some circumstances which are broader than where this is currently required. The appropriate standard was much discussed before the final text was arrived at, with the ICO noting that references in the text to both "unambiguous" consent and "explicit" consent could lead to confusion as to what type of consent was needed in a given context.

Having these two standards begs the question of when is consent "unambiguous" but not "explicit"? One way to understand the issue may be to refer to the A29WP's previous guidance on consent. The guidance frames "unambiguous" consent as that which leaves "no doubt" as to the individual's intention to deliver the consent. Nevertheless, unambiguous consent need not be express: it may be inferred from certain actions. We would suggest it is the ability for unambiguous consent to be inferred that distinguishes it from explicit consent.

The following table illustrates whether the consent in various scenarios would meet the requirements of unambiguous and/or explicit consent.

Form of consent	Unambiguous?	Explicit?
A customer contract includes a written declaration of the customer's consent to specified types of processing (the request being clearly distinguishable from other matters in the contract)	Yes	Yes
An online retailer offers customers the opportunity to opt-in to specified processing through a tick-box during the order process	Yes	Yes
At an event sign-in, participants are informed that the organisers would like to use their registration details for specified types of profiling and are asked (verbally) whether they consent to such processing	Yes, consent may be given verbally. However, the organisers may wish to consider how the consent can be documented with greater certainty, particularly in light of the GDPR's accountability requirements	
Employees are informed that photographs will be being taken in a section of the building during a particular time and that such photos will be included on the company's intranet. Employees, having been so informed, decide to go to the area in which photographs are being taken	Yes, consent may be inferred from employees' actions in going to the areas of the building in which photographs are being taken during the relevant times	No, whilst consent may be inferred from the employees' actions, it cannot be said to be explicit
A social media website requires users to provide certain personal data in order to participate on the site. The site contains a notice, accessible in the privacy section, indicating that, by using the site, users are consenting to their data being processed by third parties to deliver them marketing information	No, the GDPR is clear that inactivity cannot constitute consent. This is consistent with the "no doubt" analysis: ongoing use of the site may indicate consent to the processing, but may also mean users have not read the notice. As there is doubt as to users' intentions, ongoing use of the site cannot constitute unambiguous or explicit consent	
An online retailer offers the opportunity to opt-out of certain processing by unticking a pre-ticked box during the order process	No, as is the case under ICO guidance, the GDPR is clear that consent cannot be obtained through pre-ticked boxes	

Right to withdraw consent

The GDPR formalises the accepted position under the DPA that individuals have the right to withdraw their consent to processing. The GDPR makes it clear that withdrawal may occur at any time and individuals should be made aware of this right before giving consent. Companies will also need to ensure that it is "as easy to withdraw as to give consent". In practice, companies will likely need to allow individuals to withdraw their consent through the same medium as it was obtained and make the withdrawal process clear from the outset. It is worth highlighting that the "right of withdrawal" is considered a necessary aspect of consent: if the withdrawal right does not meet the GDPR's requirements, then consent will not have been validly obtained.

The Legitimate Interests Condition

To the relief of many companies, the changes to the legitimate interests condition are less significant than those introduced for the consent condition. As is the case under the current regime, the legitimate interests of the company or a third party may be outweighed by the individual's fundamental rights and freedoms. The GDPR adds that this is particularly the case in respect of a child and companies should, therefore, ensure that this balance has been considered and documented when relying on the condition for processing data relating to children.

However, as highlighted in the comparison above, the wording of the GDPR does not exactly track the form of the condition set out in the DPA. In general, a company's assessment of the balance between their legitimate interests and the interests of the individual will not change under the GDPR, but companies will need to carefully consider how that assessment is documented and ensure it reflects the reformulation. In particular, under the DPA a company could rely on their legitimate interests taking precedence except

Children and consent

The DPA does not expressly address the privacy of children, although non-binding guidance from various organisations sets out standards for the collection of data from children in some circumstances. For example, the Home Office Task Force for Child Protection has suggested that social networking services should put in place procedures to ensure children under the age of 13 are not able to access services, and the Information Commissioner suggests that parental consent would normally be required before collecting personal data from children under 12.

Under the GDPR, the processing of personal data of a child below the age of 16 in relation to the offering of digital services will only be lawful where consent has been given by the person holding parental responsibility. Companies are to make "reasonable efforts" to verify such parental consent, making use of available technology. The GDPR does allow Member States to lower the age limit (provided it is 13 or more) at which parental consent is required. However, to the extent that this leads to a less harmonised approach, this may present challenges for companies as website/app operators may need to implement additional jurisdictional specific procedures to account for variable age limits.

Outside the context of digital services, the GDPR requires that particular attention must be paid to the clarity and accessibility of information provided to children in relation to the processing of their data. It also anticipates that sector specific codes of conduct will continue to be relevant in protecting the interests of children.

where the processing would be unwarranted by reasons of prejudice to the individual's rights, freedoms or legitimate interests. In contrast, under the GDPR (as is currently the position under the Directive), a company must consider all interests of the individual (and not just "legitimate interests") without reference to an "unwarranted prejudice" threshold.

In its guidance on the legitimate interest condition, the A29WP makes it clear that the reference to individuals' interests, rather than legitimate interests, implies a wider scope to the protection of individuals' interests and rights. Even individuals engaged in illegal activities should not be subject to disproportionate interference with their rights. However, this does not mean that an individual's questionable, illicit interests should prevail over those of the company. Instead, the purpose of the balancing is to prevent disproportionate impact on the individual: where a company has important and compelling interests they may justify even a significant intrusion or other impact on the individual. As the GDPR mirrors the formulation in the Directive, this guidance will also be relevant in interpreting the GDPR.

Unlike the DPA, the GDPR also requires companies to consider the "reasonable expectations" of the individual, based on their relationship with the company when making their assessment of interests. In general, the more specific and restrictive the context of collection, the more limited an individual's reasonable expectations will likely be. Companies should, therefore, ensure this consideration is documented as part of the balancing assessment, discussed further below.

When will a company be able to rely on the legitimate interests condition?

As a preliminary matter, it should be remembered that, like all of the conditions with the exception of consent, the legitimate interests condition is necessity-based. That is, the condition may be relied upon only to the extent that the processing is necessary for the purpose of the company's legitimate interests. Therefore, before relying on the condition, companies should consider whether a less invasive form of processing would be available to achieve the same ends.

The GDPR and the previous A29WP guidance is clear that the assessment of whether the legitimate interests condition can be relied upon must be carried out on a case-by-case basis. However, by way of illustration, the table below sets out a number of examples of how the assessment might be made in practice.

Proposed processing	Legitimate interest?	Balance assessment
Intra-group transfer of employee/client data for administrative purposes (within the EEA)	Yes – the GDPR acknowledges that companies may have a legitimate interest in processing data in this way	Interests of the company likely to prevail as: (i) reasonable to assume employees/clients would expect their data to be processed by the group, rather than a particular entity; and (ii) company's interests appear compelling with there being little impact on the individual

Proposed processing	Legitimate interest?	Balance assessment
Market research – transferring customer data to a third party data-mining specialist processor	Likely – the GDPR acknowledges that companies may have a legitimate interest in market research activities. However, the company's interest will not be legitimate if: (i) it is not clear enough to apply the balance assessment; or (ii) it is only speculative	If the company's interests cannot be described as "legitimate", this condition may not be relied upon, even if the individual has no competing interests. The company will need to consider whether in its particular circumstances customers would expect that transfer and processing and whether that processing is likely to have a disproportionate impact
Direct marketing – promoting special offers to an existing customer via post	Yes – the GDPR acknowledges that companies may have a legitimate interest in direct marketing activities	Interests of the company likely to prevail as: (i) reasonable to assume customers would expect a business to attempt to promote its products using basic details (subject to the customer not having indicated they do not wish to receive marketing materials); and (ii) whilst the company's interests are not particularly compelling, there is relatively little intrusion into customers' privacy or other disproportionate impact. A company could strengthen this assessment by ensuring customers are given clear means to opt-out of any such marketing

Safeguards and the right to object

In its discussion of the balancing assessment, the previous A29WP guidance noted that in some circumstances it may be possible to "tip" the balance in favour of the company through the use of enhanced safeguards in relation to the proposed processing. These could include increased transparency, a general and unconditional right to opt-out of the processing and the use of technical and organisation measures to strictly limit the scope of processing. It is likely that these factors will continue to be relevant under the GDPR, though, as noted above, behaviour which was previously "best practice" is often now formally required. For example, under the GDPR, individuals have the right to object to any processing undertaken pursuant to the legitimate interests condition at any time. Once an objection has been made, the company must be able to demonstrate compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual.

Legitimate Interests: ICO guidance example

The ICO previously illustrated the balancing of interests by giving the example of a customer who has stopped making payments under a hire-purchase agreement. The customer has moved house without notifying the finance company and the ICO considers whether the company's legitimate interests in recovering the debt enable it to disclose the customer's personal data to a debt collection agency, notwithstanding that the customer has not consented to the processing and that the customer may prefer to avoid paying the debt.

The ICO's conclusion is that whilst the customer's interests may differ from those of the finance company, passing the customer's details to the debt collection agency could not be called "unwarranted". Under the GDPR, it seems likely that the conclusion in this example would be the same. However, the controller's analysis will now need to make clear that:

- in its view, the customer reasonably expected that their details might be used for the purpose of debt collection; and
- the customer's interests are not dismissed for being illegitimate, but are not compelling enough when balanced against the controller's important interests in recovering its debts to tip the balance in their favour.

Transparency

The general transparency principle requires that any information and communication relating to the processing of data (particularly the information relating to the identity of the company which is the "data controller" and the purposes of the processing) should be easily accessible and easy to understand. The GDPR then sets out more extensive, specific obligations around the type of information to be provided to individuals and the time at which it is provided. In the context of processing grounds, the GDPR provides that:

> "[At the time when personal data are obtained, controllers shall inform the data subject of:]
>
> - the purposes of the processing for which the personal data are intended, as well as the legal basis for processing;
> - where the processing is based on [the legitimate interests condition], the legitimate interests pursued by the controller or by a third party;"

The requirement to inform individuals of the legal basis for the processing (and the legitimate interests pursued, if applicable) is new to the GDPR and may prove challenging for companies to comply with.

Whilst most companies will have a sound legal basis for their processing activities, the extent to which this is documented may be more limited. Moreover, as acknowledged in A29WP guidance, the choice of the most appropriate processing ground is not always obvious and in some transactions a number of legal grounds could apply. As a result, companies may have been tempted, in the past, to seek "blanket" consent to ensure the processing is covered. Going forward, this should not even be considered an option and companies will need to spend some time assessing which grounds they are relying on.

Clearly, providing this information at the time of data collection will also prevent companies from later relying on a ground if it was not described at the time. This may be particularly relevant when companies may seek at a later date to rely on the legitimate interest condition for further processing: under the GDPR, a legitimate interest will not justify processing unless it has been described to the individual, either at the time or in a notice provided before processing on reliance of the interest commences.

Demonstrating compliance

In addition to the six processing principles, companies will, as a general matter, also be required to demonstrate how they have complied with those principles (the "accountability" principle). The GDPR provides limited direction on how a company should demonstrate compliance and we expect further guidance to be issued by the European Data Protection Board. However, as a starting point, the GDPR does indicate that compliance may be demonstrated by the adoption of internal policies and measures which promote "data protection by design" and "data protection by default", together with adherence to any approved codes of conduct and maintaining records of processing activities.

Conclusion

Some of the changes introduced by the GDPR to the consent and legitimate interests conditions merely reflect current best practice under ICO and A29WP guidance, whilst others are more significant changes. Whether or not best practice is currently followed, companies should consider reviewing the basis on which they process data to ensure that their position is "future proofed". This could involve, for example, ensuring that the form of consent obtained from individuals today will continue to be valid under the GDPR to allow processing to continue after the implementation date.

Perhaps more significantly, the GDPR's requirement that individuals be informed of the legal basis for processing will mean that companies will need to have a clear analysis of what basis is being used in different circumstances. Privacy and information notices will likely need to be amended accordingly to ensure this information is appropriately conveyed, and it may make sense to combine this process with a review to ensure notices are sufficiently clear and easy to understand, being another focus of the GDPR. Engaging with the process early should help companies with compliance with a number of the broader aims of the GDPR, such as demonstrative accountability and achieving data protection by design.

Rebecca Cousin
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Richard Batstone
T +44 (0)20 7090 3669
E richard.batstone@slaughterandmay.com

September 2016

J345675_Processing of Personal Data, consent and legitimate interests under the GDPR_v07