CRBDirect

UNDERSTANDING CONSENT POLICY

UNDERSTANDING CONSENT POLICY

The GDPR will bring changes to consent to reflect a more dynamic idea of consent, that it is an organic, ongoing and actively managed choice, and not simply a one-off compliance box to tick and file away. The definition and role of consent under the GDPR remains similar to that under the DPA. However, the GDPR builds upon the DPA's standard for consent in several areas, specifically requiring consent to be unambiguous and involve a clear affirmative action. The change may be felt greatest in its effect upon organisations consent mechanisms: Organisations will need to provide clear and more granular opt-in methods, good records of consent and simple, easy to access ways for people to withdraw consent.

Consent should be separate from other terms and conditions and organisations will require granular consent for distinct processing operations. Consent should not generally be a precondition of signing up to a service and will not be valid if obtained through pre-ticked opt-in boxes or some other method of consent by default. Organisations are required to keep clear records to demonstrate consent. Organisations must enable and appreciate an individual's right to withdraw their consent, informing them of this right and offering easy ways to withdraw consent at any time. Public authorities, employers and other organisations in a position of power are likely to find it more difficult to obtain valid consent.

Organisation will need to review existing consents and check consent mechanisms for compliance with GDPR standards. Where they satisfy those standards, there will be no need to obtain fresh consent.

The regulation defines consent in Article 4(11) as:

CRBDirect

"consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

Consent can be further broken down as:

• "consent of the data subject means any freely given" – Data subject pertains to the person whose data it relates to, further defined as an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

• "When assessing whether consent is freely given, utmost account shall be taken of whether...the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." - Where consent to processing was not strictly necessary, there is a presumption that it was not freely given. In some circumstances an organisation may successfully argue an exemption to this presumption, however this is expected to be unlikely.

Additionally, organisations seeking consent must ensure and be aware that:

• The data subject had a genuine ongoing choice and control over how their data is used. If the individual has no real choice, consent is not freely given and will be invalid;

• Consent was a positive expression of choice that was not coerced or unduly incentivized (including avoiding penalisation). This means that people must be able to refuse consent without detriment. It may still be possible, however, to incentivise consent to some extent as there will usually be some benefit to consenting to processing. For example, if joining the retailer's loyalty scheme comes with access to money-off vouchers, there is clearly some incentive to consent to marketing. The fact that this benefit is unavailable to those who don't sign up does not amount to a detriment for refusal;

• A positive expression of choice excludes pre-ticked boxes or any other methods of consent by default;

• Individuals must be enabled to withdraw consent easily and at any time; and

CRBDirect

• Consent will not be given freely if there is an imbalance in the relationship between the individual and the controller.

• *specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;" – this pertains to the data subject being fully aware without opacity that they have given their full consent either verbally or in a clear medium such as written form or via telephonic means for the data controller (means the natural or legal person, public authority, agency or other body) to collect their data; along with the purpose of why their data has been collected and exactly where it may be transferred too and what it will be used for. Organisations must clearly explain to people what they are consenting to in a way they can understand, specifically information should include;*

• The controller's identity and the identity of any third parties who will be relying on consent must be clear;

• Consent must cover all processing activities. Organisations will need to keep consents under review and refresh them if the purposes or activities evolve beyond what was originally specified. Consent will not be specific enough if details change;

• The purpose of the processing must be clear with separate consent for different processing operations wherever appropriate; Organisation must give granular options to consent separately to separate purposes, unless this would be unduly disruptive or confusing; and

• Include details of how to withdraw consent at any time.

• *Unambiguous indication - It must be obvious that the individual has consented, and what they have consented to. This requires more than just a confirmation that they have read terms and conditions – there must be a clear signal that they agree. If there is any room for doubt, it is not valid consent*

• Consent requires a clear affirmative action which requires an individual to take deliberate action to opt-in, even if not expressed as an opt-in box, this may include signing a consent statement, oral communication or a binary choice presented with equal prominence;

• Failure to opt-out is not consent;

• Consent must be verifiable. Article 7(1) makes it clear that organisations must be able to demonstrate that someone has consented.

CRBDirect

CONSIDERATIONS FOR CONSENT

• Silence, inactivity and pre-ticked boxes are not sufficient. This may mean a change in the way in which you obtain consent for marketing activities, for example, organisations that require a customer to unclick an opt-in box will not have valid consent.

• Explicit consent will continue to be required for the processing of sensitive personal data e.g. data relating to racial or ethnic origin, mental or physical health, or religious beliefs.

• Separate consents are required for different processing activities and consent must be distinguishable and can't be bundled with other written agreements. For example, where an individual signs terms and conditions that provide for multiple processing operations, but each is not distinguished clearly the individual will not have provided valid consent.

• The supply of goods and services can't be conditional on consent to processing where that processing is not necessary for the supply. So, the giving of consent for marketing cannot be a condition to, for example, booking a hotel room.

• There are greater controls over parental consents where children under 16 are asked to provide their data online. The GDPR doesn't set out the age at which a person is considered to be a child and member states are able to set their own limit provided that it is not lower than 13.