Personal data: a new age of consent

When the General Data Protection Regulation comes into force next year, companies will be obliged to demonstrate positive, unambiguous consent in order to collect and store their customers' data. The days of pre-ticked boxes are numbered – and with hefty fines for non-compliance, it's important for businesses to be prepared.

"I shall assume that your silence gives consent." From May 2018; Plato's famous words won't suffice where data-gathering and management practices are concerned. It's time you read up on the General Data Protection Regulation (GDPR).

When the Information Commissioner's Office (ICO) opened a public consultation on its draft GDPR guidance paper, it received more than 300 responses, demonstrating the importance of the issue. Going about consent properly not only benefits the individual and overall data security but is also good for strengthening consumer trust and reputation.

The GDPR comes into effect in May 2018, and the government has confirmed that the UK's decision to leave the EU will not affect adoption of the new legislation. It will impose a hefty maximum penalty – up to 4 per cent of global turnover or EUR20m, whichever is greater – for incorrectly collecting, storing or processing data. Though it is yet to be seen to what extent regulators will impose the maximum penalty, the consequences of getting consent wrong are potentially devastating.

The GDPR applies primarily to personal data, but its definition of what this means is more detailed than that described by the Data Protection Act (DPA) – and now covers things such as online identifiers, including IP addresses. Any data that would have fallen under the remit of the DPA will certainly do so under the GDPR.

The consent aspect of the legislation is about making sure that companies genuinely have permission from users to process their personal data if there is no other lawful basis for doing so. People will have real control over who does what with such information. It's about clarity and accountability and giving the individual a clear choice. Unambiguity is an abiding theme across the legislation.

Under the GDPR, when consent is relied upon as a basis for processing, it must be freely given, specific, informed and unambiguous – something that isn't always currently the case. Gone will be the days of "If you don't untick this box then you agree that we can spam you as much as we like". When it comes to consent; the ball is now very much in the court of the individual.

Any consent must be given in an affirmative, positive way and cannot be inferred. Moreover; boxes cannot be pre-ticked, the user has to tick them deliberately. Also, consent must be presented separately from other terms and conditions and mustn't form an obstacle to being able to buy something.

Any original consent given by an individual will have to be easy to rescind (meaning they will no longer have to go out of their way to do so) at any time. In fact, the GDPR states that it should be as easy to revoke consent as it was to give it in the first place.

It's likely that consent opt-out forms will become as commonplace on websites as contact forms. As soon as the individual withdraws their consent (by unsubscribing from a mailing list, by telephone or email form), this must be evidenced.

Consent is only one justification for processing personal data; there are other lawful reasons that can be relied upon such as in cases where it is necessary for data to be processed in the legitimate interests of a third party (as it is in the case of a 999 call, where you might have to give information about someone else to save your or their life), then different rules apply.

If an organisation offers an 'information society service' (such as an online helpline) to children, then it may need to obtain permission from a parent or guardian to process the child's data. Children under the age of 16 can't give that consent themselves, and so it has to come from someone with parental responsibility. The GDPR makes it very clear that this protection is especially significant when children's personal information is used for creating online profiles and marketing. However, parental consent is not required if the data processing relates to preventative or counselling services offered directly to the child.

The new legislation naturally has a bearing on how data is stored by companies. It's crucial that organisations know exactly where their data is stored should an individual wish to have it removed. They must be able to provide evidence of that data being deleted (by documenting that it has been deleted from a particular place, for example).

Consolidation of data will be integral to making this work, yet there are a surprising number of companies who don't have 100 percent certainty on where and how their data is kept. Legacy systems will need to be updated, potentially creating a large workload for many organisations. Even if the company already stores data on individuals, they need to ensure they have consent to carry on storing it, regardless of how long they may have held it.

Top tips for getting consent right

- Develop stringent selection criteria for the sensitive data that you will collect and don't rely on pre-ticked boxes
- Present your consent wording clearly, away from your other terms and conditions
- Be clear and concise at all times to avoid confusion
- Name any third parties who may rely on the consent
- Avoid having consent as a precondition of a service or offer
- Consider whether there is another lawful basis for data processing – consent should preferably be used as a last resort
- Have good data protection insurance coverage in place

QBE European Operations
Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 **QBEeurope.com**

8583/JAN/2018