

## Untying the knot—GDPR and wedding gift lists

13/08/2018

**Private Client analysis:** Hidden among the upheaval of legal preparations for the General Data Protection Regulation (GDPR) has been an unlikely shakeup in the sedentary world of wedding gift lists. Yoon Hur and Simon Miles, of Edwin Coe, explain an issue that will give lawyers cause to consider both technical compliance and broader questions of human rights and privacy.

### What risk to personal privacy do commercial online gift registries and wish lists represent?

The main risk for list owners is the ease with which these lists can be publicly accessed. On many prominent UK retailer websites, anyone can search for or even just accidentally stumble across someone's gift list, by simply searching for one named party (including name variations) or the date of an event.

Gift lists often provide a wide-ranging snapshot of people's private lives and personal tastes, which could potentially provide a resource to facilitate identity fraud or profiling, even though this would not strictly constitute personal data in the legal sense (as the prominent inclusion of say, a preferred style of crockery would not necessarily allow someone to be personally 'identified'). There is scope for the contents of these lists to come within the scope of the legislation as 'personal data', as someone's book choices on the list could indirectly indicate their religious or political beliefs, which constitute sensitive 'special categories' of data under the GDPR [Regulation \(EU\) 2016/679](#). Such data is normally afforded stricter protections and safeguards under the legislation, but this will normally be negated if the data has already been made manifestly public (by publication online).

Overly public or unwanted disclosure of gift lists can also risk reputational damage, particularly for those in the public eye—Kim Kardashian was ridiculed by media in 2011 when the gift registry for her first wedding revealed ostentatious items like a \$380 jam jar and \$7,850 vase. Under the [Data Protection Act 2018 \(DPA 2018\)](#), defined below), disclosure of personal data relating to an individual may be permitted even without the controller's consent if such disclosure is justified in the particular circumstances as being in the 'public interest' or for the 'special purpose' of journalism. This could theoretically allow information relating to a wedding list to be obtained and made public in certain circumstances, such as in the recent disclosure of several items from Prince Harry and Meghan's private wedding gift list.

There may also be issues with data retention. One prominent list provider states that they keep records of gift lists for 15 years after a wedding date to help couples easily replace items which may get broken (a good or bad thing, depending on your privacy concerns). However, while data controllers are subject to a general GDPR obligation to restrict the retention of personal data to no longer than necessary for their original purpose for processing, their privacy policies do not need to explicitly set out specific retention periods for your personal data, and many just provide some generic wording regarding the criteria used to determine this. Obviously the longer your gift list data remains 'live', the higher the risks of unwanted exposure or disclosure of its contents.

If you are a gift purchaser, being forced to buy products through sites selected by a third party rather than your usual trusted retailer may raise concerns about security over your card payment data and the general handling of your personal data. There is also a risk that if the recipient's chosen registry providers are not compliant with direct marketing and spam regulations, your purchase of a gift through these sites could end up unintentionally adding you to unwanted marketing mailing lists for their business or the retailers covered by the list, with little incentive for you to keep using the registry's services personally. Any data leak disclosing which gifts someone purchased off a list could also run a reputational risk for a purchaser if this reveals them to appear particularly ungenerous.

### What is the relevant legislation?

Three main regulations governing the privacy of personal data in the UK:

- the GDPR, which is the EU-wide regulation most readers will no doubt already be well aware of from the deluge of privacy policy and marketing consent emails that were circulated around 25 May 2018

- [DPA 2018](#), which replaces the UK's previous [Data Protection Act 1998](#) and unofficially transposes the GDPR (with a few enhancements) into UK law in preparation for Brexit
- the Privacy and Electronic Communications (EC Directive) Regulations 2003, [SI 2003/2426](#), which deal with a wide variety of electronic communications (eg websites, apps, online advertising networks), but primarily comes up in connection with website cookies and marketing emails

[SI 2003/2426](#) is based on an EU Directive which is currently under reform and expected to be replaced by a new 'e-Privacy Regulation' in the near future, although the final text for this is yet to be finalised. We expect the UK to take a similar approach to implementation post-Brexit as [DPA 2018](#) and the GDPR, although this has yet to be confirmed.

In a matter that itself might warrant further consideration, the right to respect for private and family life is also protected by the [Human Rights Act 1998](#).

## How effective is it in protecting personal information?

The focus of UK privacy laws is to provide individuals with as much clear and transparent information about an organisation's handling with their personal information as possible, so as to allow the individual to make an informed decision about whether or not they are happy to hand this data over.

The legislation sets out various general principles and obligations that controllers of personal data need to comply with, but there are no strict prescribed requirements as to what security systems or specific mechanisms need to be in place. So the onus is largely on individuals themselves to do their research (eg by reading the list provider's privacy policy) and in being proactive about choosing the gift list provider that convince them that their privacy is in the right hands—eg those that explicitly state that the list will be shut down and the user's records deleted once the list is closed, or that offer additional security settings such as requiring guests to have gift list numbers and passwords for access.

However, the legislation does expand the scope of rights individuals have in respect of seeking redress for a personal data breach or managing how their personal data is used once this is with the organisation, so retrospective redress is possible (see below).

## What redress is available to the individual if they do suffer a breach of personal privacy?

A key change under the GDPR was the expansion of individuals' rights to transparency and control over their personal data, meaning individuals can in certain circumstances request copies of all personal data held by an organisation about them, as well as request the restriction, correction, deletion or objection to further dealings with this data in certain situations. So if you wished to not only delete your gift list following the wedding but also want to make sure all personal data registered with the provider will be deleted from its records as well, you would have a legal right to request this. Organisations will normally need to comply with your request within 30 days and free of charge, although there are exceptions to both the rules regarding deadlines and fees and when the request must be complied with as well.

You can also raise complaints about an organisation's handling of your personal data to the UK Information Commissioner's Office (ICO), although the regulator will normally expect you to have tried to resolve the issue directly with the organisation first. The ICO can issue decision notices or fine an organisation for breach of its legal obligations. Separately, although an ICO finding of breach could support your case, you can make a private claim against an organisation in the courts to seek recovery of any losses and payment of compensation. Claims can be made for misuse of your data and compensation obtained for financial losses, distress and reputational damage (although in the context of gift lists this may be difficult to prove if the list has already knowingly been made publicly accessible).

## Are you aware of any recent legal developments in this area, whether in the UK or elsewhere?

We are not aware of any legal developments explicitly dealing with privacy issues regarding commercial gift registries. However, both the GDPR and [DPA 2018](#) have only recently come into force, bringing much public attention to privacy issues generally, so we may see further developments in this area in the near future.

From a human rights perspective, the European Court of Human Rights recently ruled in *Sihler-Jauch and Jauch v Germany* (2016) that a German magazine had the right to publish details about a celebrity couple's wedding despite the couple's explicit objections, and measures to restrict press coverage, as it considered the celebrity status of the couple to mean that the public had a legitimate interest in the wedding to warrant the magazine's right to freedom of expression. Published details of the wedding, such as food and catering, and photos of guests (who were not close family), were not held to be core private issues, but just generally discussed information in the context of the wedding. It could be easy to extend the application of this finding to the information contained in wedding gift lists.

*Interviewed by Julian Sayarer.*

*The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.*

FREE TRIAL