How the GDPR reforms of Data Protection laws will change Subject Access Request procedures

News - 03/04/2017

Social media, online publications and the drift of technology into more corners of our lives means that our digital footprints are constantly growing – not just in terms of the scale of the data that is held about us, but also in the number of organisations who hold it.

The EU has responded to the era of Big Data and mobile technology with new legislation that will affect anyone, anywhere, who trades in or shares data within the EU.

The new legislation – the General Data Protection Regulation (GDPR) – is the first major revision of the data protection laws for almost 20 years, and reflects the explosion in the use of technology and social media in that time. The GDPR takes effect from 25 May 2018, and will fundamentally change the relationship between the public and anyone who holds information about them – whether it's a business, a government department or a charitable organisation.

The headline changes have covered "The Right to be Forgotten" where individuals can request the erasure of personal data, mandatory reporting of data breaches to regulators within 72 hours of discovery, the appointment of qualified Data Protection officers and fines of up to 20 million euros or 4% of global annual turnover (whichever is greater) for the most serious breaches.

But there are also changes to "Subject Access Requests" (SARs) being the existing mechanism through which anyone can apply to a data controller (a government, business or charity that holds information) to see the personal data held on them.

The SAR mechanism has often been used as a pre-action discovery tool with which an individual who suspects that they have a cause for action against a data controller will make a request to gather evidence.

We were recently instructed in respect of an SAR and our client held thousands of documents in respect of the data subject, and wanted advice on how best to comply with the law.

The key points in reviewing what should be disclosed were:

- Does the document contain personal data? If a living individual cannot be identified from the data, it is not "personal data" and falls outside of the scope of the law.
- Is it reasonable to produce the data? If the production of the data would represent a disproportionate effort. (The challenge here being to make this determination the client still has to ascertain the data ie incur the effort to make that determination.)
- Where there is a significant amount of data can it be released in a summarised form.
- Data controllers must respond within 40 days of receipt of an SAR – but they may also request clarification or further information, and if they do, that "freezes the clock" until a response is received.
- Data controllers must also be alert to the possibility of anything that is being disclosed

may contain the personal data of someone else, third party data, – it would be a criminal offence to disclose a third party's personal data in a response to an SAR.

When the GDPR takes effect in late May next year, the rules around SARs will change: the definition of "personal data" will be wider and therefore will capture more information; data controllers will have only one month to respond (under the current legislation, they have 40 days in Jersey and 60 in Guernsey) but will be able to extend the period by up to two months in the case of complex or multiple requests; data controllers will no longer be able to charge a £10 administration fee but can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive; and controllers will have to say where their data came from and who it has been shared with.

By May 2018 all businesses should be ready to deal with the new SAR regime – as well as the changes covering deletion of data, reporting of breaches and the appointment of qualified Data Protection officers. Ogier's Data Protection team – including representatives from the Corporate, Banking, Employment and Regulatory teams – is ready to help.

Meet the Author

Michael Little
Counsel
Jersey
michael.little@ogier.com
T+44 1534 514374
M+44 7797 736616

Contacts

Sara Johns
Partner
Jersey
sara.johns@ogier.com
T+44 1534 514205
M+44 7797 843664

Laura Shirreffs
Associate
Jersey
laura.shirreffs@ogier.com
T+44 1534 514096

Related services

Corporate and Commercial
Channel Islands local legal services
Employment Law
Digital, Blockchain and Fintech
GDPR