Data protection in Gibraltar

Michael Nahon, a Solicitor at Hassans in Gibraltar, examines some of the areas which will affect the existing data protection regime in the British Overseas Territory of Gibraltar when the European Commission's Draft Data Protection Regulation is implemented

Gibraltar, a British Overseas Territory, is a small peninsula of approximately 6.8 square kilometres which dramatically juts out of the Spanish mainland at the entrance of the Mediterranean. With a population of approximately 30,000, it boasts a robust financial centre, underpinned by English Common Law principles in a low tax, well regulated and OECD (Organisation for Economic Cooperation and Development) compliant jurisdiction. In Gibraltar, financial services, insurance and a highly respected European focused online gaming sector, have all been allowed to thrive.

Background

The British territory is within the European Union by virtue of the accession of the United Kingdom on 1st January 1973. Gibraltar is not constitutionally part of the UK; it is part of the EU by virtue of the UK's accession. Therefore, for EU purposes, Gibraltar's membership is through the UK and it is considered a separate jurisdiction to the UK. In fact, when it comes to EU legislation, Gibraltar always has to transpose these into local law by enacting its own legislation. UK Acts of Parliament have no effect, unless specifically ratified by the Gibraltar Parliament, and this is extremely rare as the Gibraltar Parliament will, as a matter of course, pass its own legislation which is specific to Gibraltar.

Gibraltar implemented the EU Data Protection Directive 95/46 EC ('the Data Protection Directive') through its own legislation, principally the Data Protection Act 2004 ('DPA04'). There is little material difference between the data protection law in Gibraltar and the UK, as they are both designed to implement the Data Protection Directive. The most significant difference is the amount that the Information Commissioner can impose by way of fines; in the UK, it is £500,000 for serious offences, whereas in Gibraltar, the Gibraltar Regulatory Authority ('GRA') can only impose fines of up to £5000.

Due to its particularly small size, Gibraltar is proud to be able to boast an enviable 100% investigation rate of all data protection complaints made to the GRA, with each complaint being investigated in full and then subsequently determined by the GRA. As in all other jurisdictions, one of the major challenges facing the authorities in Gibraltar is keeping the law up to date and relevant compared to the rapid technological advances and current practises of the day. It is widely accepted that the original body of data protection legislation which followed the Data Protection Directive is now out of date and in need of reform.

EU Regulation

In January 2012, the European Commission published its proposals for reform in the Draft Data Protection Regulation ('the draft Regulation'). Readers will be aware that the draft Regulation is designed to replace the existing regime established by the Data Protection Directive, in an attempt to bring the law in this area up to date.

One of the aims of the draft Regulation is the harmonisation of data protection procedures and enforcement throughout the EU, as well as the adoption of a homogenous approach to ensure online privacy in the electronic communications sector.

When in force, the draft Regulation will be directly binding on all Member States including Gibraltar, without the need for further implementation measures at a national level. However, it must be noted that provision is made to allow the EU to adopt supplementary legislation where this is required.

An issue commonly encountered in practice is the question of the territorial effect of the DPA04, which largely limits its applicability to data controllers who physically operate in Gibraltar or who make use of equipment in the territory. Therefore, if a business is outside of the EU but provides goods or services into Gibraltar, under the DPA04 it is possible that no data protection legislation would apply.

Article 3 of the draft Regulation will change this so that the territorial scope of data protection legislation will now be extended to all organisations that offer goods or services into the EU.

For a small territory like Gibraltar, this represents a major improvement in practical terms of the applicability of data protection legislation. What it means is that if a business is based

outside of the EU but provides goods and services to Gibraltar, they will be caught by data protection legislation.

Another aim of the draft Regulation is the harmonisation of reporting requirements in the event of a data breach. Under the existing framework, the obligation to report data breaches varies in different countries. In Gibraltar for instance, only service providers of publically available electronic communications systems must notify the GRA (and in some instances the data subject) in the event of a data breach.

However, under Articles 30 and 31 of the draft Regulation, a mandatory requirement will be imposed on all data controllers, forcing them to notify the national data protection authority in the event of a breach. This will bring the position into line with what already exists under Gibraltar's Communication (Personal Data and Privacy) Regulations 2006 and is a significant change to current practice.

Data processors will now also need to notify their controller 'immediately after the establishment' of a breach, setting out specific information (Article 31(2)). The idea is that if a data controller subcontracts its data processing operations to a data processor, the data processor will now be bound under the draft Regulation to notify its controller, who in turn will notify the national data protection authority.

In terms of the detail which must be notified to the data protection authority (this must be done without undue delay and in any event within 24 hours of becoming aware of a breach), the notice must contain at least the following information:

- a description of the nature of the personal data breach, including the categories and number of data subjects concerned and the categories and number of data records concerned;
- the identity and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- a recommendation as to measures to mitigate the possible adverse effects of the personal data breach;
- a description of the consequences of the personal data breach; and
- a description of the measures proposed or taken by the controller to address the personal data breach.

Furthermore, if a data breach is likely to adversely affect the protection of the data subject's personal data or privacy, security breaches must be notified to the relevant data subjects without undue delay. The exception is if the controller can demonstrate that encryption or other technology rendered the data unintelligible to third parties (Article 32).

Perhaps, the biggest impact on the existing Gibraltarian data protection regime will be the introduction of serious sanctions which can be imposed against data controllers and processors.

The current sanctions provided by the DPA04 are limited to a fine of GBP2,000 (in the case of a summary conviction in the magistrate's court) or GBP5,000 (in the case of indictment in the Supreme Court). These will increase dramatically under the draft Regulation, with a maximum fine of up to €100,000,000 available for serious failures.

While national data protection authorities are left to decide the actual level of fines which should be imposed, Article 79 establishes the level of fines that can be made against controllers and processors in breach of their data protection obligations. Fines are to be set by reference to:

- the nature, gravity and duration of the breach;
- if the breach was intentional or negligent;
- the degree of responsibility of the relevant person, and any history of previous breaches;
- the technical and organisational compliance measures that were in place; and
- the degree to which the organisation has cooperated with the authorities to try and remedy the breach.

Conclusion

It remains to be seen whether the draft Regulation will be implemented in full in its current format or whether it will be modified further. However, it is clear that the mandatory reporting requirements together with the tough sanctions that can now be imposed make it extremely risky for any business to ignore its data protection obligations in full. This can only be seen as a positive development for the jurisdiction's overall reputation as a robust finance centre.

Michael Nahon
Hassans
michael.nahon@hassans.gi