THE OFFICE OF THE
Data Protection Commissioner

The Data Protection Commissioner's response to the proposed amendment of Regulation of Investigatory Powers Law (RIPL) – Retention of Communications Data.

The Commissioner is grateful for the opportunity to comment on the proposed amendments to RIPL relating to the retention of communications data.

As highlighted by the Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, this issue is of considerable importance to all citizens.

Freedom and confidentiality of correspondence and all other forms of communication are among the pillars of modern democratic societies. Their inviolability has been specifically safeguarded in the European Convention on Human Rights which Jersey has reflected within the Human Rights (Jersey) Law 2000.

This proposal is, for the first time, aiming to introduce obligation to retain, for investigation purposes, vast amounts of data relating to the communications of any and all citizens. Currently, such data are not stored or else are retained only on a temporary basis by electronic service providers – and if so, exclusively for contractual purposes.

Traffic data interferes with the fundamental right to confidential communications guaranteed by Article 8 of the Human Rights Law. In a democratic society, any interference with this right can be justified if it is necessary in the interests of national security.

The European Court of Human Rights has stressed that secret surveillance poses a danger of undermining or even destroying democracy on the ground of defending it; additionally the Court has affirmed that States may not, in the name of national security, adopt whatever measures they deem appropriate.

This is why any restrictions of this fundamental right must be based on a pressing need, should only be allowed in exceptional cases and be the subject of robust safeguards. The retention of traffic data – including location data – for purposes of law enforcement should meet strict conditions, in particular it must take place only for a limited period and when necessary, appropriate and proportionate in a democratic society.

The powers available to law enforcement agencies in the fight against terrorism must be effective, but they cannot be unlimited or misused. A proportionate balance must be struck to ensure that we do not undermine the kind of society we are seeking to protect. This balance is especially necessary when requiring communication service providers to store data that they themselves have no need for.

We are of the opinion that the argument is yet to be made evidencing the need for a communications service provider to retain data routinely for national security purposes, for any longer than the data would normally be retained for its own business purposes.

It is the view of this office that the use of a voluntary code of practice in these circumstances has severe limitations. It is hard to reconcile the claims made for the importance of continued retention of communications data for the safeguarding of national security with the reliance on the voluntary co-operation of service providers. If there is a need for such retention, we would prefer this to be on the basis of a statutory duty which would provide a greater degree of certainty than is possible with this voluntary arrangement.

It is also of some concern that this data is to be retained by ISP's who are not – as far as I am aware - specifically regulated and have no security standards to adhere to covering areas such as the storage of data, management, access controls etc.

There are a number of matters of significance that require detailed discussion including questions relating to the proposed retention periods and access to the retained data. We are therefore grateful for the inclusion of 29C (3)(a) within the amendment requiring the Minister to consult with this office on the code of practice.

Emma Martins
Data Protection Commissioner **Sept 07**