P.2017/26

PROPOSTIONS

COMMITTEE *for* HOME AFFAIRS

DATA PROTECTION: EU GENERAL DATA PROTECTION REGULATION

The States are asked to decide:-

Whether, after consideration of the policy letter entitled 'Data Protection: EU General Data Protection Regulation' dated 13 March 2017, they are of the opinion:-

1. To direct the preparation of legislation for the purposes of implementing provisions equivalent to the GDPR and the Law Enforcement Directive in the Bailiwick;

2. To direct the Committee to report back to the Assembly with detailed proposals in relation to the Data Protection Supervisory Authority and the sources of funding for the Authority in the third quarter of 2017.

The above Propositions have been submitted to Her Majesty's Procureur for advice on any legal or constitutional implications in accordance with Rule 4(1) of the Rules of Procedure of the States of Deliberation and their Committees.

P.2017/26

COMMITTEE *for* HOME AFFAIRS

DATA PROTECTION: EU GENERAL DATA PROTECTION REGULATION

The Presiding Officer
States of Guernsey
Royal Court House
St Peter Port
Guernsey

13th March, 2017

Dear Sir

1. Executive Summary

1.1. The purpose of this Policy Letter is to bring forward proposals to the Assembly for the preparation of new Bailiwick of Guernsey Data Protection legislation which is aligned to the EU General Data Protection Regulation ("GDPR") and the Directive relating to the Processing of Personal Data for the purposes of the Prevention of Crime ("Law Enforcement Directive"). The legislation is intended to enable the Bailiwick to demonstrate, in due course, that it is a jurisdiction which provides an adequate level of protection for personal data in accordance with the standards set out in the GDPR and for the purposes of the Law Enforcement Directive.

1.2. Key terms used within this Policy Letter include the following:-

- "Data Controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
- "Data Processor" means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;
- "Data subject" means an individual who is the subject of the personal data;
- "Personal data" means any information relating to an identified or identifiable natural person;
- "Natural person" means a living individual;
- "Processing" means obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data;
- "Data breach" means a breach of security leading to the accidental or

unlawful destruction, loss, alteration, unauthorised disclosure of personal data;

- "Special category data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, criminal convictions and offences, genetic or biometric data for the purpose of uniquely identifying an individual, data concerning health or sexual orientation;

- "Data protection adequacy" means that there is a satisfactory level of protection of personal data equivalent to that within EU Member States.

2. Background

2.1. In September 2016 the Committee *for* Home Affairs provided the Assembly with an update on the European Union ("EU") General Data Protection Regulation ("GDPR") and proposed the reappointment of Mrs. Emma Martins as Data Protection Commissioner for the Bailiwick of Guernsey under the Data Protection (Bailiwick of Guernsey) Law, 2001. Agreement was granted to extend the appointment of the Commissioner until December 2018 to ensure that the expertise of the Office is maintained, and to secure continued pan-Island working.

2.2. The Committee *for* Home Affairs also made the commitment to return to the States of Deliberation in the first quarter of 2017 (and has endeavoured to return as soon as was possible) with proposals for new data protection legislation, which would both enhance the Bailiwick of Guernsey's current data protection regime, ensuring that Bailiwick citizens are afforded the same privacy rights as EU citizens, and also ensure that adequacy is granted by the European Commission to allow the continued free flow of personal data into and out of the Bailiwick from EU Member states.

2.3 In view of the tight time-table for drafting the necessary Bailiwick-wide legislation (which is intended to come into force in May 2018, or as soon as possible thereafter), the Committee considers it necessary to submit the general proposals in this Policy Letter in order to obtain the States' approval for the necessary regulatory legislation to be drafted to implement provisions equivalent to the GDPR and the Law Enforcement Directive in the Bailiwick.

3. New Data Protection Legislation

3.1. New EU legislation was published in May 2016 which will replace the existing 1995 Data Protection Directive ("the 1995 Directive") from May 2018. The legislation

consists of two legal instruments, the General Data Protection Regulation[1] ("GDPR") and a Directive relating to the processing of personal data for the purposes of the prevention of crime[2] ("the Law Enforcement Directive"). Guernsey currently has data protection adequacy recognised by the EU due to the Data Protection (Bailiwick of Guernsey) Law, 2001 which gives effect to the 1995 Directive, and Guernsey will need to obtain equivalence status under the new GDPR if it wishes to continue freely to access EU markets.

3.2. The GDPR has the principle of extraterritoriality. In practical terms, this means that the GDPR covers personal data related to any EU citizen, regardless or not of whether it is processed within the EU. As such these EU changes will significantly impact other jurisdictions, including the Channel Islands. The GDPR will generally allow the transfer of EU citizens' data only to jurisdictions where the EU believes adequate standards of data protection are in place, meaning that jurisdictions that process data on EU citizens must achieve or maintain "adequacy status" in order to be assured of being able to continue to process such data.

3.3. The GDPR provides the Bailiwick of Guernsey with an opportunity to not only ensure that adequacy standards are met to continue to process the data of EU citizens, but to also afford all Islanders with the equivalent level of privacy rights as EU citizens through the enactment of new data protection legislation.

3.4. The Universal Declaration of Human Rights [3](UDHR) provides a common standard of achievements for all peoples and all nations and encompasses within its principles the right to privacy. This fundamental right to privacy is regarded by many as being particularly important in the digital age. In supporting the digital sector, it is important to ensure that there are appropriate standards which enable the sector to develop successfully whilst providing adequate protection for the privacy of individuals.

3.5. To this end, and following extensive consultation with the Island's Business Sectors and colleagues in the States of Jersey, it is recommended that there should be a new Bailiwick of Guernsey Data Protection Law to replicate the GDPR as closely as possible whilst ensuring that any economic advantages are incorporated if

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[3] Universal Declaration of Human Rights proclaimed by the United Nations General Assembly on 10 December 1948.

appropriate, and so as not to risk the Bailiwick's adequacy status.

3.6. This report provides a summary of key changes that would be required in the new law under the following headings:

1. The Data Protection Principles
2. Data Subject's Rights
3. Controller and Processor Responsibility
4. Breach Notification
5. Transfer of Data Overseas
6. Data Protection Officers
7. Administrative Fines
8. Supervisory Authority

1. THE DATA PROTECTION PRINCIPLES

1. The six data protection principles set out in Chapter II Article 5 of the GDPR are as follows:

Personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject (**lawfulness, fairness and transparency**);

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (**purpose limitation**);

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**);

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**);

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject (**storage limitation**);

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

2. In addition to the Chapter II Article 5 principles, the GDPR implements a "principle of accountability" under which the controller shall be responsible for, and be able to demonstrate, compliance (**accountability**).

2. DATA SUBJECT'S RIGHTS

It is proposed to strengthen a data subject's right in relation to both access to data and use of personal data. In accordance with the GDPR increased data subject's rights would include the following provisions:

- Right of access to the personal data being processed;
- Right to rectification of inaccurate personal data;
- Right to erasure of personal data when it is no longer required or when consent is withdrawn (when consent has provided the basis for processing);
- Right to restrict processing when accuracy is contested or when the controller no longer needs the personal data for the purposes of processing;
- Right to data portability and to transmit data to another controller without hindrance;
- Right to object unless the controller demonstrates compelling legitimate grounds.

Exemptions will apply where the controller can demonstrate legitimate grounds which override the data subject interest, rights and freedoms or for the establishment, exercise or defence of legal claims.

3. CONTROLLER AND PROCESSOR RESPONSIBILITY

A significant change within the GDPR is that it places direct obligations on data processors. It is proposed that data processors (entities who process personal data on behalf of a data controller) should be obliged to comply with particular data protection requirements which previously only applied to data controllers (entities who determine why and how personal data are processed). These obligations should include, but are not limited to:

- Accountability of personal data processing activities carried out on behalf of a controller;

- Consultation and cooperation, on request, with the supervisory authority in the performance of its tasks;

- Restrictions on enlisting sub-processors or replacing a processor without the authorisation of the controller;

- Appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

- Breach notification to the controller without undue delay upon becoming aware of a data breach. (Data subjects will also be able to claim compensation for unlawful processing of their personal information).

4. BREACH NOTIFICATION

Under the current data protection legislation, there is no legal requirement to report to the Data Protection Commissioner a personal data breach. Under any new Bailiwick of Guernsey Data Protection legislation it is proposed that in accordance with the GDPR, a controller will be placed under an obligation to notify the Supervisory Authority (explained below in section 8) of the breach within 72 hours of becoming aware of it.

5. TRANSFER OF DATA OVERSEAS

In the context of the GDPR Guernsey is regarded as a third country, whereby the transfer of personal data may take place where the European Commission ("the Commission") has decided that the third country ensures an adequate level of protection. Such transfers then, would not require any specific authorisation.

When assessing the adequacy of the level of protection, the Commission will take into account the rule of law, the existence and effective functioning of the Supervisory Authority and the international commitments of the third country.

In the absence of an adequacy decision a controller or processor would only be able to transfer data to a third country where appropriate safeguards are provided or effective legal remedies for data subjects are available. This would require the implementation of a number of solutions including legally binding and enforceable instruments or binding corporate rules which would place excessive obligations on the organisations involved.

6. DATA PROTECTION OFFICERS

In accordance with the requirements of the GDPR, new Bailiwick of Guernsey Data Protection legislation would impose upon Bailiwick organisations an obligation to appoint a data protection officer (DPO) if the organisation:

- Is a public authority (except for courts acting in their judicial capacity);

- Carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or

- Carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

A single data protection officer may be appointed to act for a group of companies or for a group of public authorities, taking into account their structure and size.

Any organisation will be able to appoint a DPO, regardless of whether the GDPR obliges them to do so or not, however an organisation must ensure that it has sufficient staff and skills to discharge the obligations under the GDPR.

The tasks of the DPO are as follows:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;

- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; training staff and conducting internal audits;

- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

7. ADMINISTRATIVE FINES

In order to strengthen the enforcement of appropriate levels of data protection in accordance with the GDPR, it is proposed that any new legislation will provide for penalties including administrative fines which may be imposed for infringements of the law. In order to ensure harmonisation of administrative fines across EU Member States and third countries, and to prevent the loss of Guernsey's adequacy status, penalties should be consistent with those of EU Member States and should take account of the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility, and previous relevant infringements and the manner in which the Supervisory Authority became aware of the infringement. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards, including effective judicial safeguards (e.g. appeals).

8. SUPERVISORY AUTHORITY

The current data protection law provides for a general obligation to notify the processing of personal data to the Supervisory Authority, however in many cases

this does not contribute to the improvement of protection of personal data. As such, the GDPR states that general notification requirements should be abolished and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons, by virtue of their nature, scope, context and purpose. With the loss of the revenue accrued from notification fees, Guernsey's Supervisory Authority, the Office of the Data Protection Commissioner (ODPC), will be required to operate with an alternative funding model.

The ODPC implements, and ensures compliance with, the current Data Protection Law. However, while the regulator operates autonomously from the government in practice under the current data protection regime, reform will be required to provide the degree of structural independence expected of a Supervisory Authority pursuant to the GDPR. Further, while the Commissioner is provided with a number of regulatory and enforcement powers within the current Law, additional powers will be required under new data protection legislation in order to provide equivalent protection for data subjects in accordance with the standards set out in the GDPR.

The States of Guernsey and States of Jersey have jointly commissioned a piece of work to analyse the resources that will be required by the ODPC in order to implement and enforce the GDPR effectively. Subject to the outcomes of this work, it is anticipated that the regulator should be able to generate its own income, with a view to becoming either wholly or partly self-funding, once the revenue stream that it currently obtains from general notification fees falls away.

Additionally, the consultant has been asked to recommend a range of value-added services that the ODPC might deliver to organisations in Guernsey and Jersey, beyond its minimum obligations, to encourage best practice for processing personal data in the Islands, ensuring that citizens are educated of their rights, and organisations are supported in meeting their obligations.

3.7. It is proposed that the Committee report back to the Assembly with detailed proposals in relation to the Data Protection Supervisory Authority and the sources of funding for the Authority in the third quarter of 2017.

4. "Law Enforcement Directive"

4.1. The processing activities by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences , including the safeguarding against and the prevention of threats to public security and the free movement of such data, is subject to Directive (EU) 2016/680 ("Law Enforcement Directive").

4.2. Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities is crucial in order to ensure effective judicial cooperation in criminal

matters and police cooperation. To that end, it is proposed that the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data by competent authorities should be equivalent to that in EU Member States.

4.3. Effective protection of personal data requires the strengthening of the rights of data subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data.

4.4. The Directive requires that clear distinction is made between personal data of different categories of data subjects, such as:

a) Persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

b) Persons convicted of a criminal offence;

c) Victims of a criminal offence or persons with regards to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

d) Other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

4.5. Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent law-enforcement authorities from carrying out activities such as covert investigations or video surveillance, as long as they are laid down by law and constitute a necessary and proportionate measure with due regard for the legitimate interests of the natural person concerned.

4.6. The Directive expresses that natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular:

- The specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data;

- The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. In order to ensure

that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review;

- The competent authorities should ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available.

4.7. Implementation of the rules laid down by the Directive in the Bailiwick of Guernsey will enable Law Enforcement agencies to continue to work cooperatively with EU Members States without the need for additional arrangements and protocols to be established. This will promote the continued flow of information where there is a need for cross-border collaboration.

4.8. Implementation of the Directive will also demonstrate to other non-EU countries that Guernsey is a well-regulated jurisdiction with high data protection standards within Law Enforcement.

4.9. The Directive places an obligation on Member States to ensure that transfers of personal data to a third country take place where the Commission has decided that the third country ensures an adequate level of protection for personal data (see Article 36). Consequently for the purposes of the Directive, the Bailiwick will be subject to an adequacy decision by the European Commission, taking into account:

- The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law, as well as the implementation of such legislation, data protection rules, professional rules and security measures;

- The existence and effective functioning of the independent supervisory authority in the third country or to which an organisation is subject;

- The international commitments the third country or organisation concerned has entered into.

5. Consultation

5.1. With proposed changes to local data protection legislation, it has been, and will continue to be, absolutely vital to engage with all of the Island's citizens and business sectors. This has been undertaken in a number of different ways and has included the formation of a number of industry working parties, GDPR briefing events, consultancy workshops, extensive one-to-one engagement and public communication through local media outlets.

5.2. The first phase of industry working parties took place in November and December 2016 and focussed specifically on the proposed new data protection legislation.

There is a high level of commitment from the local business sectors who have identified the need for Guernsey to adopt the GDPR. The second phase of industry working parties is due to be held in March 2017, following the completion of the consultancy work, and will focus on the regulatory regime.

5.3. The first GDPR briefing event held in October 2016 attained a very high turnout and level of engagement. Briefing events will continue to be scheduled throughout 2017 and 2018 to ensure that the public and business communities are kept appraised as the project progresses. Extensive one-to-one engagement has also been undertaken, including attendance and presentation delivery at a large number of forums.

5.4. Consultation has been, and will continue to be, undertaken with the Office *of the* Policy and Resources Committee and the Office *of the* Committee *for* Economic Development.

5.5. Consultation with Alderney and Sark is due to commence in conjunction with the legislative drafting process.

6. Conclusions

6.1. The GDPR represents the biggest global change in data protection in well over a decade and is a regulation that is relevant to every organisation, irrespective of size or sector. Accountability is at the heart of the changes with an increased expectation that organisations will be able to demonstrate compliance and ensure that the rights of data subjects are met.

6.2. Although there will inevitably be an increase in compliance obligations (for all implementing or aligning with the GDPR), this data protection reform provides Guernsey with a number of economic opportunities, particularly in creating a well-regulated, compliant jurisdiction with highly trained and experienced data protection professionals; an environment which is increasingly attractive for those organisations who understand the value of quality regulation. Key to achieving this is by ensuring that adequacy status is granted by the European Commission, through the enactment of new data protection legislation which provides an adequate level of protection in accordance with the GDPR and Law Enforcement Directive and which will allow the continued transfer of personal data between the Bailiwick and EU Member States.

7. Recommendations

7.1. In the circumstances of this report, the Committee *for* Home Affairs recommends the States:-

a) To direct the preparation of legislation for the purposes of implementing provisions equivalent to the GDPR and the Law Enforcement Directive in the Bailiwick;

b) To direct the Committee to report back to the Assembly with detailed proposals in relation to the Data Protection Supervisory Authority and the sources of funding for the Authority in the third quarter of 2017.