Bloomberg Law® Privacy & Data Security

Country Profile: GUERNSEY

Richard Field, of Carey Olsen, Guernsey, provided expert review of the Guernsey Country Profile and wrote the Risk Environment section. [Last updated July 2017. – Ed.]

I. APPLICABLE LAWS AND REGULATIONS

The principal piece of legislation governing privacy and data security in the Bailiwick of Guernsey is the Data Protection (Bailiwick of Guernsey) Law, 2001, effective Aug. 1, 2002 (DPL). Guernsey will have a new data protection law, designed to implement the provisions of the General Data Protection Regulation, which will come into force in May 2018. However, this note reflects the law as it currently stands in Guernsey.

Under the DPL, data controllers must adhere to specified requirements concerning how the personal data of data subjects is processed, maintained, and transferred. The DPL is applicable to all data controllers that are established in Guernsey and to data controllers that use data processing equipment in Guernsey for purposes other than transferring the data through Guernsey (Sec. 5(1), DPL). Data controllers in the latter category must nominate a legal representative established in the Bailiwick (which includes the islands of Guernsey, Alderney, Herm, and Sark) (Sec. 5(2), DPL).

The law defines a "data controller" as any person who determines the purpose for which, and the manner in which, personal data of data subjects is to be processed. "Personal data" is data relating to a living individual who can be identified from that data or from the data combined with other information in the possession of the data controller (Sec. 1(1), DPL). In addition, the law identifies specific categories of "sensitive personal data," including data containing information regarding the data subject's race or ethnicity, political opinions, religious beliefs, union membership, mental or physical health or condition, and sex life, as well as any information on the actual or alleged commission of a criminal act or any criminal proceedings or convictions (Sec. 2, DPL).

In addition to the DPL, Orders and Regulations issued by the States of Guernsey and guidance published by the Office of the Data Protection Commissioner (DPC; see below) impose obligations on data controllers and/or provide benchmarks for "best practice." A list of these Orders and Regulations is available through the "Legislation" tab on the DPC Guidance page, and they are specifically referenced as relevant below.

A. Data Protection Principles

Under the DPL, data controllers must comply with the following eight principles governing the processing of personal data:

1. personal data must be processed fairly and lawfully;
2. personal data must be collected only for one or more specified and lawful purposes;
3. personal data must be adequate, relevant, and not excessive in relation to its purpose;
4. personal data must be accurate and up-to-date;
5. personal data must be kept for no longer than necessary for the intended purpose;

6. personal data must be processed in accordance with the data subject's rights under the DPL;

7. the data controller must take appropriate technical and organizational measures against unauthorized or unlawful processing as well as any accidental damage, loss, or destruction of personal data; and

8. the data controller may not transfer personal data to a country outside the European Economic Area unless that country has an adequate level of protection for the rights of data subjects.

(Schedule 1, DPL, implementing Secs. 4(1)-(2), DPL).

B. Personal Data Processing

Data controllers may only process personal data if one of the following requirements is met:

- the data controller has the consent of the data subject;
- the processing is necessary for the performance of a contract to which the data subject is a party, or for taking steps at the request of the data subject to facilitate the subject's entering into a contract;
- the processing is necessary to comply with a legal obligation of the data controller (other than a contractual obligation);
- the processing is necessary to protect the vital interests of the data subject;
- the processing is necessary for the administration of justice or to the performance of public functions; or
- the processing is necessary for the purposes of legitimate interests pursued by the data controller or the third party to whom the data is disclosed.

(Schedule 2, DPL, implementing Sec. 4(3), DPL).

More stringent requirements must be met prior to processing a data subject's sensitive personal information, including at least one of the following:

- the data subject has given “explicit” consent (as opposed to the general consent requirement above, which may be tacit or implied under some circumstances);
- the processing is necessary for exercising or performing a legal right or obligation imposed on the data controller in connection with employment;
- the processing is necessary to protect the vital interest of the data subject or another person where explicit consent cannot be given and the data controller cannot reasonably be expected to obtain it, or where the consent of the data subject has been unreasonably withheld;
- the processing is carried out by a non-profit association that has met specified requirements;
- the data subject has made the information public;
- the processing is necessary for legal proceedings, obtaining legal advice, or establishing, exercising, or defending legal rights;
- the processing is necessary for the administration of justice or for specified public functions;
- the processing is necessary for specified medical purposes and is undertaken by a health professional or other person owing a duty of confidentiality to the data subject; or
- the processing involves racial or ethnic origin information used to review the existence or absence of equal opportunity or treatment for such persons, provided that appropriate safeguards are in place.

(Schedule 3, DPL, implementing Sec. 4(3), DPL).

In addition to these requirements, the Data Protection (Processing of Sensitive Personal Data) Order, 2002 (Sensitive Personal Data Order), issued by the States of Guernsey and effective the same date as the DPL, permits processing of sensitive personal data under a number of other circumstances, including when necessary to prevent unlawful acts, when necessary to protect against or publish information about

malpractice or mismanagement, or when the information concerns other issues such as disclosures for journalistic, artistic, or literary purposes; counselling services; insurance and pension determinations and processing; discrimination issues related to religion or physical or mental health status; research in the general public interest; or processing necessary to the functions of a police officer (Paras. 1-9, Sensitive Personal Data Order).

C. Notice, Access, and Correction

In general, the DPL confers a number of rights on data subjects in Guernsey. Specifically, data subjects have the right to be informed by the data controller whenever personal data about them is being processed by or on behalf of the data controller. In such circumstances, the data subject is entitled to a detailed description of the personal data, the purpose of the processing, and the recipients to whom the personal data may be disclosed, as well as a communication, in intelligible form, of the information itself and its source. In addition, if the processing is being conducted through automated processing means for evaluative purposes (*e.g.*, assessing the data subject's performance at work, creditworthiness, etc.) and that evaluation is likely to constitute the sole basis of a decision regarding the data subject, the data subject is entitled to be informed regarding the logic employed by the data controller in the decision-making process (Sec. 7(1), DPL).

The Data Protection (Miscellaneous Subject Access Exemptions) Order, 2002 (Subject Access Exemptions Order), issued by the States of Guernsey and effective the same date as the DPL, further exempts specified adoption records and reports from DPL access requirements (Secs. 1 and Schedule, Part I, Subject Access Exemptions Order).

It should be noted, however, that a data controller is not obligated to provide any of the information outlined above unless the data subject has submitted a written request for the information, together with any fee required by the data controller (Sec. 7(2), DPL). The maximum fee generally allowed to be charged is £10 (Sec. 2, Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations, 2002 (Fees Regulations)), with fees regarding access requests made of credit reference agencies limited to £2 (Sec. 3, Fees Regulations). In addition, under specific provisions of the Fees Regulations amended in 2010, the maximum fee allowed to be charged for access to health records delivered by means other than paper (*i.e.*, electronically or on CD) is £50, and for paper health records, the fee is capped at £10 for 10 pages, £50 for up to 100 pages, and £0.50 for each additional page above 100 (Sec. 1, Data Protection (Subject Access) (Fees and Miscellaneous Provisions) (Amendment) Regulations, 2010 (2010 Fees Amendment Regulations); see also "Guidance on Subject Access to Health Records," DPC, September 2015).

If the data controller requires further information to confirm the identity of the data subject making the request, it may withhold the requested data until the identifying information is provided (Sec. 7(3), DPL). Finally, if a data controller cannot comply with a request without disclosing information related to another person, the data controller may refuse the request unless the other person has consented to the request or it is reasonable to comply with the request without the other person's consent, as defined by the law. However, this provision does not excuse a data controller from providing as much information as possible without disclosing the other person's identity (Sec. 7(4)-(6), DPL).

The DPL specifies that the data controller must respond to a data subject's request within 60 days of receiving it or, if further information is required, within 60 days of the receipt of the required fee and the additional information (Sec. 7(11), DPL).

If a court is satisfied upon the application of a data subject that his personal data is inaccurate, the court may order the data controller to rectify, block, erase, or destroy that data, together with any other data that contains an expression of opinion that the court believes to be based on the inaccurate data. In some circumstances, the court may also order the data controller to inform third parties of the rectification, blocking, erasure, or destruction (Sec. 14, DPL).

D. Exemptions

Personal data is subject to exemption from some or all of the requirements described in subsections B and C above under the following circumstances, as specified more fully in the DPL:

- when required for national security (Sec. 28, DPL);
- when processed for the purposes of crime detection or tax assessment (Sec. 29, DPL);

- when exempted by the States of Guernsey for the sake of health, education, or social work (Sec. 30, DPL);
- when exempted for the sake of regulatory activity, such as charities, protection against financial loss, or practices contrary to fair trading (Sec. 31, DPL);
- when exempted for the sake of journalism, literature, or art (Sec. 32, DPL);
- when exempted for the sake of research, history, or statistics (Sec.33, DPL);
- information publicly available by enactment (Sec. 34, DPL);
- disclosures required by law or made under legal proceedings (Sec. 35, DPL);
- data processed for purposes of the data subject's personal, family, or household affairs (Sec. 36, DPL); and
- miscellaneous exemptions under DPL Schedule 6 (Sec. 37, DPL).

E. Other Individual Rights

In addition to the general notice, access, and correction rights described above, data subjects in Guernsey have rights regarding the processing of personal data in the following circumstances:

- A data subject may serve notice in writing to a data controller requiring it to stop or modify the processing of any personal data on grounds that the processing is likely to cause substantial and unwarranted damage or distress to the data subject (Sec. 10(1), DPL). This provision does not apply if the data subject has consented to the processing or if the processing is necessary for the performance of a contract, compliance with a legal obligation, or in the vital interest of the data subject (Schedule 2, DPL).
- In addition to the requirement that a data subject may request to be informed of the logic regarding a decision made concerning the subject via automatic processing means (see subsection C, above), a data subject may serve notice in writing to a data controller requiring that no such decision may be based solely on automated processing (Sec. 12(1), DPL).
- A data subject may serve notice in writing to the data controller requiring it to cease, or not to begin, processing personal data for purposes of direct marketing (Sec. 11(1), DPL).

In each of the above instances, the law specifies the time within which data controllers must comply with the notice, as well as court intervention for failure to comply (Secs. 10-12, DPL).

Data Management

Retention

According to the fifth data protection principle under the DPL, personal data “shall not be kept for longer than is necessary” for the specified purpose. DPL Schedule 1, Part 1(5).

A guidance note prepared jointly by Guernsey's Office of the Data Protection Commissioner and Jersey's Office of the Information Commissioner provides that personal data should be kept indefinitely “only in exceptional circumstances.”

Localization

Guernsey does not have a data localization law, but the eighth data protection principle under the DPL prohibits the transfer of personal data to a country or territory outside the Bailiwick “unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.” DPL Schedule 1, Part 1(8). There are also a number of mechanisms (such as EU Model Clauses, Binding Corporate Rules, and Privacy Shield) by which international transfers can be effected. Further, there are exemptions to the general rule, including obtaining the data subject's consent and processing undertaken pursuant to the performance of a contract to which the data subject is a party. It should be noted that Guernsey is considered “adequate” by the European Commission, and as such international transfers to and from Guernsey into the EU are *prima facie* lawful.

Disposal

Other than the fifth data protection principle, which provides that personal data "shall not be kept for longer than is necessary," no provision under the DPL specifically mandates disposal of personal data. However, the aforementioned guidance note provides that data controllers should have in place a procedure for the removal of different categories of data after certain periods, "for instance, when the information is no longer required for audit purposes or when a client no longer requires your services."

II. REGULATORY AUTHORITIES AND ENFORCEMENT

The DPL is administered by the Office of the Data Protection Commissioner (DPC). This office is concurrent with the Office of the Information Commissioner of the Bailiwick of Jersey and is held by the same individual. The duties of the DPC are outlined in Article 6 of the DPL. In its latest Annual Report for 2015, published in August 2016, the Commissioner notes that the recently enacted EU General Data Protection Regulation does not require data controllers to notify the Commissioner regarding data processing or to pay a fee (see below), which is a source of concern to be monitored by the Commissioner going forward. Operating income from notification fees and state sources totaled just over £200,000 for the 2014 calendar year (p. 22, Annual Report).

The DPC handles relatively few complaints (just 37 in 2015) but has seen an increase in recent times. The number of data controller notifications has also increased in recent years. There were no enforcement actions issued in 2015 (pp. 11-15, Annual Report); the DPC prefers to take a collaborative approach, designed to ensure lessons are learned and best practice integrated.

A. Required Notifications by Data Controllers

Data controllers are required to register with the DPC prior to processing any personal data. The notification must provide specified information about the data controller and a general description of the measures it will take to ensure that data is not unlawfully processed or accidentally lost, destroyed, or damaged (Secs. 16-18, DPL). In addition, a data controller must notify the Commissioner whenever any of its information has changed or if it has modified its compliance measures (Sec. 20, DPL).

The fee for filing an initial notification with the Commissioner is £35, and an annual fee of £35 applies to retention of an entry in the Commissioner's registry of notifications (Secs. 6 and 12, Data Protection (Notification and Notification Fees) Regulations, 2002 (Notification Regulations)). The regulations provide additional guidance with respect to the notification requirements outlined above.

Tools for data controllers to file online notifications or update existing notifications are available on the DPC website.

B. Enforcement Provisions

Part 5 of the DPL outlines the primary enforcement mechanisms available to the DPC. If the Commissioner determines that any of the data protection principles are being violated, an enforcement notice may be served on a data controller. The Commissioner must consider whether a violation has caused damage or distress to the data subject. The notice may include instructions regarding rectification, blockage, erasure, or destruction of personal data under specified circumstances, as well as any required third party notification (Sec. 40, DPL).

A data subject (or another person acting on the subject's behalf) may request the Commissioner to make an assessment as to whether processing is being carried out in compliance with the DPL. In such instances, the Commissioner must make the assessment and respond to the data subject as to the results of the assessment and any view formed or action taken (Sec. 42, DPL). The Commissioner may issue an information notice to a data controller if it does not have the information necessary to conduct the assessment (Sec. 43, DPL). Specific rules apply to the Commissioner's determination as to whether personal data is being processed for "special purposes" (*i.e.*, journalistic, literary, or artistic material) (Secs. 44-46, DPL). The DPC does not possess the power to issue fines, but failure to comply with an enforcement notice issued by the DPC is a criminal offense (Sec. 47, DPL).

Any person who processes personal data in contravention of the notification requirements (Sec. 21, DPL), fails to comply with an enforcement or information notice or knowingly or recklessly makes a false

statement in connection with such a notice (Sec. 47, DPL), or unlawfully obtains personal data without the consent of the data controller (Sec. 55, DPL) commits an offense under DPL. If prosecuted, such persons are subject to fines up to Level 5 of the Uniform Scale of Fines (Sec. 60(1)-(2), DPL), which translates to £10,000. See Uniform Scale of Fines (Bailiwick of Guernsey) Law, 1989, Sec. 1(2).

Finally, an individual suffering damage by reason of a contravention of the DPL is entitled to compensation from the data controller for such damage (Sec. 13(1), DPL), and an individual suffering from distress due to a contravention may also be entitled to compensation, but only if such individual either suffered damage as described above or if the contravention relates to processing of personal data for journalistic, artistic, or literary purposes (Sec. 13(2), DPL).

III. RISK ENVIRONMENT

Guernsey's data protection regime has been recognized by the European Commission as providing an adequate level of protection for personal data. This “adequacy” status is vital in today's digital economy to ensure the future success of the Island as a trusted financial center, hence the unsurprising decision to follow the EU's lead and overhaul the current law. Guernsey's government has adopted the stance that it wishes Guernsey to be at the forefront of data protection regulation, much as it is in terms of FATCA, CRS, AML, and other forms of regulatory compliance.

Guernsey will therefore be bringing into force a new data protection law in May 2018, largely mirroring the provisions of the GDPR (with some necessary local adaptations). While the precise interaction between the GDPR and the new Guernsey law has still to be determined, businesses can expect that the standards being applied in Guernsey will be similar to those across the EU. This will mean some significant augmentation to the local regime, but in the main, it will be an evolution of the core principles and legislation that currently apply.

Under the current regime, the DPC does not have the power to issue fines and adopts a collaborative approach to issues that are identified. The number of complaints made on an annual basis is small, and enforcement action is infrequent and of a minor nature. It is difficult to say whether the low number of complaints is a consequence of businesses adopting a high standard in terms of data protection, but the position will come under much greater scrutiny in May 2018 when the new law comes into effect (along with the GDPR).

While the new regime will bring significant fining powers to the DPC and an increased scrutiny over data protection practices, the collaborative approach will remain. The focus of the regulator will be on education and prevention, rather than punishment. That is not to say that the fining (and other) powers will not be used; rather, these will likely be used less frequently, at least until “best practice” is established and further guidance from both local and EU regulators is at hand.

While there are currently provisions attributing criminal liability to certain acts/omissions relating to data protection, we are not aware of any such cases being brought, certainly not in the last decade. There is a private right of action against a company that breaches the legislation and causes distress and damage; however, we are not aware of any judgments being issued in respect of such claims. It is likely that this position will change as consumer awareness increases, compliance with automatic breach reporting highlights some common failings, and there is greater scrutiny on the operation of the regime by EU regulators, keen to ensure that GDPR standards are being applied.

Cybersecurity continues to be an important part of all data protection programs, and it is notable that there has been a real focus on this area in recent times. The use of technology as a disruptor in traditional financial services markets means that Guernsey has to be innovative, while meeting international standards, and it is anticipated that we will see significant activity in these areas in the coming years.

IV. EMERGING ISSUES AND OUTLOOK

A. Commissioner Urges Diligence in Preparation for GDPR

In a January 2017 release, the DPC called on Guernsey businesses and other stakeholders to ensure that they are prepared for the changes to be implemented by the EU General Data Protection Regulation (GDPR) when it becomes effective in May 2018. The Commission announced that it will prepare information and guidance on the GDPR throughout 2017 to assist businesses in their compliance with the new regulation ("Businesses Urged to Prepare for Major Overhaul of Data Protection Law Due in 2018," Office of Data Protection Commissioner, Jan. 27, 2017). Further information concerning the effect of the GDPR on Guernsey and the plan to draft legislation to comply with its provisions is available at the DPC website and via its new GDPR-specific portal.

B. Proposed Revision to Data Protection Law

On March 13, 2017, Guernsey's Committee for Home Affairs released a Policy Letter proposing changes to the Data Protection Law so as to align it with the GDPR (EU/2016/679) and the EU Directive on Processing Personal Data for Law Enforcement Purposes (EU/2016/680). It is expected that the draft law will be finalized in the coming months, released in October, and debated at local government level in November. It is thereafter anticipated that the new law will come into force in May 2018 to coincide with the GDPR being applied across the EU. For more information, see Commentary from Carey Olsen, or send an e-mail to richard.field@careyolsen.com or cigdpr@careyolsen.com to obtain a copy of the firm's *Channel Islands Guide to the General Data Protection Regulation*.

