Bloomberg Law | Privacy & Data Security

Workplace Privacy Requirements: GUERNSEY

Richard Field, of Carey Olsen, Guernsey, provided expert review of the Guernsey Workplace Privacy Requirements. [Last updated July 2017. – Ed.]

100. WORKPLACE PRIVACY — INTRODUCTION

The principal piece of legislation governing privacy and data security in the Bailiwick of Guernsey is the Data Protection (Bailiwick of Guernsey) Law, 2001 (DPL).[1] 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 or that use data processing equipment in Guernsey for purposes other than transferring the data through Guernsey. Data controllers in the latter category must nominate a legal representative established in the Bailiwick (which includes the islands of Guernsey, Alderney, Sark, and Herm) (Sec. 5, 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 (Sec. 1(1), DPL). Accordingly, employers generally are considered to be data controllers subject to DPL requirements regarding adherence to data protection principles, processing of personal data, and the rights of data subjects to notice, access, and correction, as outlined more fully below.

The DPL is administered by the Office of the Data Protection Commissioner (DPC).[2] This office is concurrent with the Office of the Information Commissioner of the Bailiwick of Jersey and is held by the same individual.

300. BACKGROUND CHECKS

300.10. Laws and Regulations Governing Background Checks

Key laws and regulations include:

- Data Protection (Bailiwick of Guernsey) Law, 2001 (DPL)[3];
- Data Protection (Processing of Sensitive Personal Data) Order, 2002 (Sensitive Personal Data Order)[4];

[1] Data Protection (Bailiwick of Guernsey) Law, 2001, Apr. 29, 2002, http://www.guernseylegalresources.gg/article/94296/Data-Protection-Bailiwick-of-Guernsey-Law-2001.

[2] Office of the Data Protection Commissioner, https://dataci.gg/.

[3] Data Protection (Bailiwick of Guernsey) Law, 2001, Apr. 29, 2002, http://www.guernseylegalresources.gg/article/94296/Data-Protection-Bailiwick-of-Guernsey-Law-2001.

[4] Data Protection (Processing of Sensitive Personal Data) Order, 2002, States Advisory and Finance Committee, Aug. 1, 2002, http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=73379&p=0.

- Data Protection (Miscellaneous Subject Access Exemptions) Order, 2002 (Subject Access Exemptions Order)[5];
- Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations, 2002 (Fees Regulations)[6];
- Data Protection (Subject Access) (Fees and Miscellaneous Provisions) (Amendment) Regulations, 2010 (2010 Fees Amendment Regulations)[7];
- Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 (Rehabilitation of Offenders Law)[8];
- Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 (Commencement, Exclusions and Exceptions) Ordinance, 2006 (2006 Exceptions and Exclusions Ordinance)[9];
- Population Management (Guernsey) Law, 2016 (Population Management Law)[10]; and
- Population Management (Employment Records) Regulations, 2017 (Employment Records Regulations).[11]

A complete list of all orders and regulations promulgated under the DPL is available through the "Legislation" tab on the DPC Guidance page.

300.20. Information Collection

300.20.10. Information Collection — In General

"Personal data" is defined as 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). Under the DPL, data controllers must comply with the following eight principles governing the collection and processing of personal data:

- Personal data must be processed fairly and lawfully;
- Personal data must be collected only for one or more specified and lawful purposes;
- Personal data must be adequate, relevant, and not excessive in relation to its purpose;
- Personal data must be accurate and up-to-date;
- Personal data must be kept for no longer than necessary for the intended purpose;
- Personal data must be processed in accordance with the data subject's rights under the DPL;
- 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

5 Data Protection (Miscellaneous Subject Access Exemptions) Order, 2002, States Advisory and Finance Committee, Aug. 1, 2002, http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=73382&p=0.

6 Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations, 2002, States Advisory and Finance Committee, Aug. 1, 2002, http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=73386&p=0.

7 Data Protection (Subject Access) (Fees and Miscellaneous Provisions) (Amendment) Regulations, 2010, Home Department, June 24, 2010, http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=72335&p=0.

8 Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002, June 17, 2002, http://www.guernseylegalresources.gg/article/98586/Rehabilitation-of-Offenders-Bailiwick-of-Guernsey-Law-2002.

9 Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 (Commencement, Exclusions and Exceptions) Ordinance, 2006, July 1, 2006, http://www.guernseylegalresources.gg/article/98587/Rehabilitation-of-Offenders-Bailiwick-of-Guernsey-Law-2002-Commencement-Exclusions-and-Exceptions-Ordinance-2006.

10 Population Management Law, 2016, April 3, 2017, available at http://www.guernseylegalresources.gg/article/154337/Population-Management-Guernsey-Law-2016.

11 Population Management (Employment Records) Regulations, 2017, April 3, 2017, available at http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=107089&p=0.

- 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).

Processing requirements: 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 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).

The DPL provides for a variety of exemptions from some or all of the requirements under specified circumstances, such as if processing is required for national security, for crime or tax collection purposes, and for a host of other exemptions, as outlined in Part 4, Secs. 27-39 of the DPL. To the extent that these exemptions impact specifically in the context of an employment situation, they are specified in this discussion.

Sensitive personal data: The law specifies 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). More stringent requirements must be met prior to processing a data subject's sensitive personal data, 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;
- 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 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 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).

300.20.20. Information Collection Restrictions

300.20.20.10. Financial Information

Employers in Guernsey routinely request credit report information concerning applicants for employment. Any information obtained as a result of a pre-employment credit check would qualify as personal data under the DPL, and the employer is obligated to follow Guernsey data protection principles and requirements regarding processing, access, and correction (see 300.20.10, 300.30, and 300.40).

300.20.20.20. Criminal History

Employers in Guernsey commonly request applicants and employees to submit a Basic Disclosure document from the Guernsey Police as part of the recruitment and selection process. The Basic Disclosure contains information regarding any unspent convictions and cautions with respect to the job candidate. A Basic Disclosure is generally requested in person and requires a photo ID and a £20 fee. In addition, applicants may file a Subject Access Request as permitted under Section 7 of the DPL for a full copy of all the applicant's convictions and cautions, which requires verified identification and a £10 fee. Information on how to obtain these documents is contained on the Guernsey Police website.

The Guernsey Rehabilitation of Offenders Law provides that an individual convicted of certain offenses will be rehabilitated (meaning, essentially, that the conviction is no longer considered a part of the individual's record) if the individual has not been reconvicted for a specified period of time and other conditions are met (Sec. 1, Rehabilitation of Offenders Law). Generally, individuals are not required to disclose any such "spent" conviction to a prospective employer as part of the application process (Sec. 7(3), Rehabilitation of Offenders Law). However, in certain circumstances, the 2006 Exceptions and Exclusions Ordinance requires disclosure of spent conviction information, including cases where the question is asked of an applicant seeking employment in certain professions (i.e., medical practitioner, lawyer, accountant, etc.) (Sec. 1 and Schedule 1, 2006 Exceptions and Exclusions Ordinance), in a position working with children or vulnerable adults (Sec. 4 and Schedule 3, 2006 Exceptions and Exclusions Ordinance), or in certain positions in the finance and banking industry (Sec. 5 and Schedule 4, 2006 Exceptions and Exclusions Ordinance).

In practice, particularly with respect to positions working with children and vulnerable adults, employers will conduct a direct check with the UK's Disclosure and Barring Service (DBS), conducted through the Guernsey Vetting Bureau (GVB). A DBS check will include information on both unspent convictions and on spent convictions that nevertheless must be disclosed under the 2006 Exceptions and Exclusions Ordinance. Step-by-step information on applying for a DBS check is available from the GVB's Information and Compliance Manual.[12]

Under the UK Employment Practices Data Protection Code,[13] which the DPC has indicated that it will follow in most circumstances, employers should delete any information concerning an applicant's criminal conviction once the information has been verified unless the information is clearly relevant to the ongoing employment of the employee (Sec. 1.7.4, Employment Practices Data Protection Code).

Any information obtained by an employer as a result of a criminal background check qualifies as personal data under the DPL, and the employer is obligated to follow Guernsey data protection principles and requirements regarding processing, access, and correction (see 300.20.10, 300.30, and 300.40).

300.20.20.30. Driving Records

Employers in Guernsey may conduct a background check concerning an applicant's driving record, provided that it is relevant to the prospective job duties of the applicant. Any information obtained by an

---

12 "Information and Compliance Manual," GVB, August 2014, https://www.gov.gg/CHttpHandler.ashx?id=92618&p=0.

13 Employment Practices Data Protection Code, https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf.

employer as a result of a driving records check qualifies as personal data under the DPL, and the employer is obligated to follow Guernsey data protection principles and requirements regarding processing, access, and correction (see 300.20.10, 300.30, and 300.40).

To the extent that a position is connected with a road service license under the Guernsey Public Transport Ordinance, 1986, applicants are obligated under the 2006 Exceptions and Exclusions Ordinance to disclose any spent convictions regarding the refusal, suspension, or revocation of a PSV license or badge (Sec. 3(c) and Schedule 1, Part III, para. 4, 2006 Exceptions and Exclusions Ordinance).

300.20.20.40. Work History and Educational Background

There are no specific Guernsey provisions regulating the collection of information regarding the work history or educational background of an applicant or employee. In practice, employers conduct checks to verify such information to confirm the identity of applicants and to assess their suitability for the position at issue. Any information obtained by an employer as a result of a work history or educational background check qualifies as personal data under the DPL, and the employer is obligated to follow Guernsey data protection principles and requirements regarding processing, access, and correction (see 300.20.10, 300.30, and 300.40).

300.20.20.50. References

The DPL's treatment of employment references distinguishes between references that have been given by an employer and references that are received by an employer. Employers are not obligated to provide a copy of a reference that the employer has written about an employee (Schedule 6, para. 1, DPL). However, there is no similar provision with respect to references that the employer has received from another party. In such cases, if an employee requests access, the employer must consider the request, taking the normal rules of access under the DPL into account. Employers may consult the entity that provided the reference to ascertain any reasonable confidentiality concerns, but should provide access in most circumstances.[14]

300.30. Notice of Information Collection

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 (i.e., 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 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).

300.40. Access to, and Correction of, Information Collected

In general, an employee must submit a written request and pay any fee required by the data controller to gain access to his personal data (Sec. 7(2), DPL). In general, the maximum fee allowed to be charged is £10 (Sec. 2, 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 and Miscellaneous 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

[14] "Good Practice Note: Subject Access and Employment References," Office of the Data Protection Commissioner, https://www.dataci.je/wp-content/uploads/2016/05/GPN-SAR-Employment-References_May16.pdf.

additional page above 100 (Sec. 1, 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). 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).

300.50. Employment Verification Requests

There are no specific provisions in Guernsey governing employment verification requests. Any information obtained by an employer as a result of an employment verification request qualifies as personal data under the DPL, and the employer is obligated to follow Guernsey data protection principles and requirements regarding processing, access, and correction (see 300.20.10, 300.30, and 300.40).

500. HEALTH INFORMATION, MEDICAL EXAMINATIONS, AND DRUG AND ALCOHOL TESTING

500.10. Health Information — In General

All information concerning an employee's health is considered to be "sensitive personal data" under the DPL, and employers therefore must abide by the law's requirements concerning processing, access, and correction of such data (see 300.20.10, 300.30, and 300.40). Of particular importance in the health context, an employer should ensure that it has the explicit consent of the data subject, that it collects only information that is absolutely necessary, and that it keeps all health information secure.

The Guernsey Office of the Data Protection Commissioner has indicated that it will follow the approach to data protection regarding worker health information outlined in Part 4 of the UK Employment Practices Data Protection Code. The Code outlines core principles regarding worker health information, including information from medical examinations, drug and alcohol testing, and genetic testing, as outlined more fully below.

500.20. Pre-Employment Health Questions

Guernsey employers are permitted to ask applicants about health issues during the recruitment and selection process. Any data collected for such purposes is considered to be "sensitive personal data" under the DPL, and employers therefore must abide by the law's requirements concerning processing, access, and correction of such data (see 300.20.10, 300.30, and 300.40).

Pre-employment health questions must be relevant to the position at issue. The Employment Practices Data Protection Code indicates that employers should only obtain medical information through testing of applicants where there is a likelihood that an offer will be made and that any testing is necessary and justified to determine the applicant's fitness (Sec. 4.3.2, Employment Practices Data Protection Code).

500.30. Medical Examinations

Many Guernsey employers provide for periodic medical examinations for their employees. Information collected under these circumstances is considered to be "sensitive personal data" under the DPL, and

employers therefore must abide by the law's requirements concerning processing, access, and correction of such data (see 300.20.10, 300.30, and 300.40).

In general, data collected from employee medical examinations should be relevant and necessary to the employee's job responsibilities. The Employment Practices Data Protection Code specifies that information should only be obtained if it is part of a voluntary occupational safety and health program or if it is necessary to: (a) prevent a significant safety risk to the employee or others; (b) determine the employee's fitness to begin or return to the assigned duties; or (c) determine entitlement to benefits (Sec. 4.3.3, Employment Practices Data Protection Code).

Information obtained in the course of an employee medical examination that is not relevant in determining the above factors should be permanently deleted by the employer (Sec. 4.3.4, Employment Practices Data Protection Code).

500.40. Drug and Alcohol Testing

Employers are permitted to conduct drug and alcohol testing of applicants and employees. Any data collected as a result of such testing is considered to be "sensitive personal data" under the DPL, and employers therefore must abide by the law's requirements concerning processing, access, and correction of such data (see 300.20.10, 300.30, and 300.40).

Prior to obtaining information through drug or alcohol testing, an employer should ensure that the benefits of such testing outweigh any adverse impact. Accordingly, testing is generally justified only for health or safety reasons. Post-incident testing based on reasonable suspicion of abuse is more likely to be justified than random testing, and where possible, random testing should be limited to employees working at "safety-critical" activities (Secs. 4.4.1 and 4.4.4, Employment Practices Data Protection Code).

500.50. Genetic Data

Genetic testing of employees is rare in Guernsey. Any data collected as a result of such testing is considered to be "sensitive personal data" under the DPL, and employers therefore must abide by the law's requirements concerning processing, access, and correction of such data (see 300.20.10, 300.30, and 300.40).

The Employment Practices Data Protection Code specifically suggests that genetic testing should not be used to obtain information predictive of an employee's future general health and strongly discourages asking an employee for the results of any previous genetic testing (Secs. 4.5.1 and 4.5.2, Employment Practices Data Protection Code). Genetic testing should only be used to obtain information in cases where it is clear that the employee displays a particular, detectable genetic condition that is likely to pose a serious safety risk or where the relevant work environment is known to cause risks to employees with particular genetic characteristics. Even under these circumstances, employers should use such testing only as a last resort after considering changes to work environment or practices (Sec. 4.5.3, Employment Practices Data Protection Code).

700. EMPLOYEE MONITORING AND SURVEILLANCE

700.10. Employee Monitoring and Surveillance — In General

Under most circumstances, employee monitoring in Guernsey will be considered intrusive, and any employer wishing to conduct such monitoring must balance the privacy expectations of its employees against the employer's right to monitor its business systems and to ensure that its business interests are protected (see, i.e., Sec. 3.1, Employment Practices Data Protection Code). Monitoring and surveillance policies generally are spelled out in employment contracts or in policy documents issued by the employer. To the extent that an employer spells out the activities being monitored and the purpose of the monitoring, it will be deemed to have employee consent, and the monitoring will be permitted.

Any data collected as a result of employee monitoring and surveillance is considered to be "personal data" under the DPL, and in many instances, such monitoring and surveillance will result in the collection of "sensitive personal data." Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, and 300.40).

The Guernsey Office of the Data Protection Commissioner has indicated that it will follow the approach to data protection regarding monitoring at work outlined in Part 3 of the UK Employment Practices Data Protection Code. The Code outlines core principles regarding workplace monitoring and surveillance, including electronic communications, video monitoring, and location monitoring, as outlined more fully below.

700.20. Electronic Communications

Any data collected as a result of employer monitoring of its employees' electronic communications, such as e-mail, is considered to be "personal data" under the DPL, and in many instances, such monitoring will result in the collection of "sensitive personal data." Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, and 300.40).

Under the Employment Practices Data Protection Code, employers should establish an e-mail usage policy and communicate it to employees prior to the implementation of any monitoring (Sec. 3.2.1, Employment Practices Data Protection Code). Employers also should consider the extent to which they may limit monitoring of electronic communications to the level necessary to ensure system security and whether an automated system is sufficient to the purpose (Sec. 3.2.3, Employment Practices Data Protection Code). Further, an employer should consider whether benefits justify the adverse impact of e-mail monitoring and, if such monitoring is conducted, should avoid opening e-mails, particularly e-mails appearing to be private or personal (Sec. 3.2.7, Employment Practices Data Protection Code). Finally, employees should be informed of the retention period for their e-mail information (Sec. 3.2.11, Employment Practices Data Protection Code).

700.30. Internet

Any data collected as a result of employer monitoring of its employees' Internet usage is considered to be "personal data" under the DPL, and in many instances, such monitoring will result in the collection of "sensitive personal data." Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, and 300.40).

Most of the best practices regarding appropriate monitoring of electronic communications under the Employment Practices Data Protection Code are equally applicable to employees' use of the Internet, including establishing a usage policy, limiting monitoring to the extent possible, and informing employees regarding the retention of their Internet usage data (see 700.20). Employers should clearly specify any restrictions on what materials may be viewed on, or copied from, the Internet, including examples as appropriate (Sec. 3.2.1, Employment Practices Data Protection Code).

700.40. Video Monitoring

Any data collected as a result of video monitoring by an employer is considered to be "personal data" under the DPL, and in many instances, such monitoring will result in the collection of "sensitive personal data." Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, and 300.40).

While Guernsey does have a Guidance Document[15] regarding the data protection concerns arising out of the use of CCTV equipment, by its own terms this guidance does not apply to the use of surveillance techniques by employers to monitor their employees' compliance with contracts of employment (Guidance Document, pg. 1).

Under the Employment Practices Data Protection Code, employers should consider whether the benefits of video monitoring of employees justify the adverse impact on employee privacy. In general, video surveillance should be limited to areas of particular risk where the expectation of privacy is low (Sec. 3.3.1, Employment Practices Data Protection Code). In addition, employers should clearly notify employees and any others (such as customers or visitors) that monitoring is being conducted and should specify the location and purpose of the monitoring (Secs. 3.3.2 and 3.3.3, Employment Practices Data Protection Code). The Code specifies that employers using covert monitoring should do so only in extreme circumstances and should ensure that it is targeted to obtaining evidence of malpractice and

15 "CCTV Guidance for Users," DPC, August 2007, https://www.dataci.gg/wp-content/uploads/2015/03/CCTV.pdf.

criminal activity within a set time frame and is discontinued after completion of the investigation, among other limits (Sec. 3.4, Employment Practices Data Protection Code).

700.50. Location Monitoring

Employers may choose to monitor the location of employees through vehicle movement tracking or other GPS-based technologies. Any data collected as a result of employer location monitoring is considered to be “personal data” under the DPL, and in many instances, such monitoring will result in the collection of “sensitive personal data.” Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, and 300.40).

Under the Employment Practices Data Protection Code, employers should consider whether the benefits of in-vehicle monitoring justify the adverse impact. Specifically, employers should establish a policy outlining permissible private use of employer-provided vehicles and should ensure that employees are informed with respect to the policy and any monitoring activity conducted to enforce it (Sec. 3.5, Employment Practices Data Protection Code).

700.60. Telephone Use

Any data collected as a result of employer monitoring of employee telephone use is considered to be “personal data” under the DPL, and in many instances, such monitoring will result in the collection of “sensitive personal data.” Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, and 300.40).

If telephone calls or voice mails are monitored, employers should consider whether the benefits of monitoring outweigh the adverse impact and, if they do, should inform employees accordingly, including an acknowledgment that some personal messages may be heard. When possible, employers should consider whether using itemized call records would be sufficient to the purpose of the monitoring (Sec. 3.2.4, Employment Practices Data Protection Code).

700.70. Searches and Inspections

There are no Guernsey laws or regulations specifically addressing employer searches and inspections of employees. To the extent that an employer conducts a search or inspection, any data collected as a result is considered to be “personal data” under the DPL, and in many instances, such a search or inspection will result in the collection of “sensitive personal data.” Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, and 300.40).

700.80. Biometrics

There are no Guernsey laws or regulations specifically addressing the collection and processing of employee biometric data such as fingerprints, iris scans, or face recognition data. To the extent that an employer collects such information, it is considered to be “personal data” under the DPL, and in many instances, such collection will constitute the collection of “sensitive personal data.” Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, and 300.40).

900. PERSONNEL RECORDS

900.10. Personnel Records — In General

Personnel records maintained by employers are subject to collection, processing, access, and retention requirements under the DPL, the Population Management Law, and the Employment Records Regulations. In general, personnel records are considered to be “personal data” under the DPL and, in many instances, will constitute “sensitive personal data.” Accordingly, employers must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, 300.40, and below).

The Population Management Law requires all employers, including self-employed persons, to keep records containing information specified by regulation (Sec. 35, Population Management Law; see also Reg. 1(1), Employment Records Regulations). Any employer failing to keep such records is guilty of an offense and subject to a fine of up to Level 4 on conviction (Sec. 48, Population Management Law).

The Employment Records Regulations specify the types of information that must be included in employee records for each employee, including name; date of birth; social security number; and the reference number, expiry date, and any conditions imposed on the employee's Certificate, Permit, or old regime (right to work) document (Reg. 1(1), Employment Records Regulations). These rules also apply to self-employment records (Reg. 1(2), Employment Records Regulations).

An employer must keep any employment records at (or in such a way that they can be inspected from) its principal place of business in Guernsey, or by entering that information on the Employer Portal accessed via the population management pages of the States of Guernsey website. Employers must meet specified record maintenance requirements if not using the Employer Portal, including keeping them together in such a way that facilitates the identification of every employee and making them capable of being reproduced in legible form and (where there are more than 30 employees) in alphabetical order or with an alphabetical index.

The Employment Practices Data Protection Code provides guidance for employers with respect to best personnel record practices, including maintenance, security, access, and retention (Part 2, Employment Practices Data Protection Code).

900.20. Access to, and Correction of, Personnel Records

In general, an employee must submit a written request and pay any fee required by the data controller to gain access to his personal data, including personnel records (Sec. 7(2), DPL; see 900.30, below). 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 (Secs. 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).

The Employment Records Regulations provide that employers must notify the Administrator within 28 days of an employee's employment ceasing if it is using the Employer Portal (Reg. 4, Employment Records Regulations). Similar rules apply to self-employed individuals.

900.30. Fees for Access to Personnel Records

The DPL provides for the imposition of a fee to be paid to the data controller by the data subject for access to the subject's personal data, including personnel records (Sec. 7(4), DPL). In general, the maximum fee allowed to be charged is £10 (Sec. 2, 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 and Miscellaneous 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, 2010 Fees Amendment Regulations; see also "Guidance on Subject Access to Health Records," DPC, September 2015).

900.40. Retention of Personnel Records

Under the DPL, personal data should be kept only for as long as it is necessary for the intended purpose, although it does not provide for specific retention periods. However, under the Employment Records

Regulations, employers may destroy an employee record at any time following the 28th day after the date when employment ceased (Reg. 3, Employment Records Regulations).

However, it is standard practice for employers to retain personnel records for a period equivalent to the relevant prescription period (the Guernsey equivalent of a limitation period)—in other words, for six years (plus a few months in case claims issued shortly before the period expired are served later). It is anticipated that there will be further guidance on this issue in due course, noting that the Population Management Law has only recently come into force.

Guidance on retention practices can be found in the Employment Practices Data Protection Code. Specifically, the Code recommends that employers destroy pre-employment recruiting records as soon as possible but no later than six months after they are collected (Sec. 1.7.2, Employment Practices Data Protection Code). With respect to personnel records, employers should only retain information that is still needed and should establish standard retention periods for categories of information applicable to all employees. In addition, employers should anonymize the records when possible and should delete any information concerning criminal convictions (see 300.20.20.20) once the conviction is spent under Guernsey law. Finally, employers should ensure that any record destruction is carried out securely and effectively (Sec. 2.15, Employment Practices Data Protection Code).

900.50. Disclosure of Personnel Data to Third Parties

Under the DPL, any processing of personal data must be necessary for the purposes of legitimate interests pursued by the data controller or the third party to whom the personal data is disclosed (Schedule 2, para. 6, DPL). Because information contained in personnel records is considered personal data (and may be considered “sensitive personal data” in some circumstances, such as records regarding medical information), employers transferring information to a third party must follow Guernsey data protection principles and requirements regarding processing, access, and correction of such information (see 300.20.10, 300.30, 300.40, and below).

In addition, the Eighth Data Principle of the DPL provides that data may not be transferred to a party in a country outside the European Economic Area unless the country or territory ensures an adequate level of protection with respect to the rights of data subjects (Schedule 1, Part 1, para. 8, DPL). The law defines what constitutes an “adequate level of protection” (Schedule 1, Part 2, para. 13) and provides for exceptions under specified circumstances (Schedule 1, Part 2, para. 14 and Schedule 4, paras. 1-9, DPL).

Further, sections 36-39 of the Population Management Law provide for confidentiality of records maintained pursuant to that law, together with exemptions for disclosure in certain circumstances. It is a criminal offense to breach those confidentiality provisions (Sec. 49, Population Management Law).

