The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the **Law**")

General Advice & Guidance for States Members

INTRODUCTION

The Data Protection (Bailiwick of Guernsey) Law, 2017 ('the Law') regulates the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information, and the purposes for which that information is used or held in connection with. The type of information covered by the Law can be as little as a name and address. The Law gives enforceable rights to individuals (data subjects) and places obligations on those persons who control the manner and the purpose of the processing of personal data (controllers), including the need to complete a registration with the Office of the Data Protection Authority (the ODPA).

The ODPA recognises the important role played by all elected representatives and the associated need to ensure that citizens have trust and confidence in those who may be handling their information. This document aims to assist States Members to understand more about data protection and provide some practical advice about what steps may be required to achieve compliance with the Law and accompanying Regulations.

High standards of data governance are important for the Bailiwick and its social and economic success. We are proud of the work done to ensure our regulatory regime is effective, citizens are empowered and protected, and businesses are supported and informed.

With data such a vital element of our daily lives, you are encouraged to explore the way in which the Bailiwick approaches its responsibilities by visiting the website of the ODPA where you will find information, including events, podcasts and newsletters aimed at raising awareness and engagement throughout our community. If you are on LinkedIn, you may wish

to consider connecting with the ODPA to get updates on news stories and other relevant information.

If you need particular help regarding registration, interpretation or application of the Law, please contact the ODPA, who will be glad to assist.

IS THERE A NEED TO REGISTER?

Acting on behalf of a Committee?

In considering whether there is a requirement to register, Members must decide in which capacity they intend to process personal data.

States Members who sit on a Committee, are likely to have access to and process personal data held at departmental level. In such a situation, the controller is the service area rather than the member. The service area is, therefore, legally responsible for the information, for compliance with the Law and potentially liable for any breach.

Acting on own behalf?

If Members process personal data to act on their own behalf, they are likely to have to register in their own right. Examples include the processing of personal data in order to timetable surgery appointments or progress complaints or enquiries made by local residents.

Any Member who is unsure of whether or not they need to register should contact the ODPA for further advice.

2021 changes

After agreement by the States of Guernsey to move the ODPA to a self-funded status, the registration regime will be changing from 2021. The ODPA will provide updates on its website in advance of these changes coming into effect.

THE DATA PROTECTION PRINCIPLES

The Law requires controllers to comply with the **seven data protection principles** when processing personal data. Ensure you understand what each principle requires and how that impacts you in your role.

If you process data as part of Committee activities, they are the controller and therefore responsible for ensuring the principles are complied with.

If you process data in your own right as a controller, you need to ensure that you understand and comply with the principles.

1. Lawfulness, Fairness and Transparency

Processing of personal data is **lawful** only if a valid condition for processing can be relied upon. For special category data, at least one of the conditions in Part II or III of Schedule 2 must be satisfied. For the processing of any other personal data at least one condition in Part I or II of Schedule 2 must be satisfied. Ensure you are clear about which condition or conditions you are relying on. More detailed guidance can be found here.

Fair processing relates to the method in which the personal data is obtained, including whether any person from whom it is obtained is deceived or misled as to the purpose or purposes for which it is to be processed. Ensure that you think carefully about how you collect information from people.

Transparency of processing is achieved by ensuring that information is given to people l at the time of collection explaining how their personal data is to be used including how long it is to be retained for, to whom it may be disclosed or transferred, together with reference to the rights they have over their data. More detailed guidance is available here.

TOP TIPS

- Understand your processing in detail.
- Establish and document which condition you are relying on for all processing involving personal data and special category data.
- Ensure you provide all necessary information to data subjects.

Case Study 1:

The Electoral Roll is prepared by the Registrar-General of Electors. It contains personal data relating to those Bailiwick residents who are eligible to vote and must only be used for election purposes.

There is a requirement within the accompanying legislation that the Electoral Roll be made available for inspection at Sir Charles Frossard House and the Guille-Alles Library. Copies of the register can also be given to persons standing for election once the nominations have been made.

It is not permitted for a States Member to either inspect the data or obtain copies of the data for purposes other than public elections, for example, to establish the address of a constituent in relation to a dispute between two parties. To do so would constitute unfair processing and would breach the first principle.

2. Purpose Limitation

Personal data must be collected for a specific, explicit and legitimate purpose and once collected must not be processed in a manner incompatible with that purpose or those purposes.

TOP TIPS

- Establish and document the purpose for which you process all personal data and special category data.
- Ensure a full data protection compliance review is conducted if that purpose changes.

Case Study 2:

A States Member holds personal data of the members of his/her Committee, plus the details of many of his constituents on his computer for the purposes of discharging his duties as a government official.

This States Member also has a new business selling CDs and DVDs on-line. He has the e-mail addresses of Committee members and of most of his constituents and decides it would be a good business drive to send out marketing e-mails to all the people on his database to drum up some new business. He gets no reply so sends them out again. He continues to do this every day until the next meeting.

At the next meeting, all the members complain about receiving these e-mails and ask him to stop. The States Member has clearly breached the second principle as he is using data

collected in one role for another, unconnected purpose.. He would need to register his company separately and wear his company 'hat' to market people. Even then, he would need consent from his constituents and colleagues before processing their data in this manner.

3. Minimisation

Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

TOP TIP

- Only hold data that you need and make sure you provide the required detail to the data subject about why you need their data and how you intend to process it.

Case Study 3:

A States Member held personal details of an individual claiming housing welfare. In order to pursue the claim, all that was needed from the individual was their name, address and date and place of birth. The States Member, however, asked the individual to provide personal details far in excess of what was required to pursue the claim.

This would constitute a breach of this principle as any personal data requested by the States Member from the individual must be relevant for the purposes of the claim, and not excessive for those purposes.

4. Accuracy

Personal data must be accurate and where applicable, kept up to date, and reasonable steps must be taken to ensure that personal data that is inaccurate (having regard to the purpose for which it is processed) is erased or corrected without delay.

TOP TIPS

- Think about how you will ensure data you process are accurate and put procedures in place to review accuracy where appropriate.
- Make it easy for data subjects to review and correct their data.

Case Study 4:

The accuracy of the Electoral Roll can only be guaranteed by the Registrar-General of Electors who has the responsibility of maintaining that data. People move house regularly, and it is fair to assume that it would take very little time for the register to become inaccurate and out of date.

It is for this very reason that the onward processing of data obtained from the Electoral Roll can be dangerous, whether or not that data has been obtained fairly and lawfully.

5. Storage Limitation

Personal data must not be kept in a form that permits the identification of a data subject any longer than is necessary for the purposes for which it is processed.

TOP TIPS

- Identify and document retention periods for all personal data you process and put in place procedures to implement those.
- Ensure data destruction methods are appropriate and secure.

Case Study 5:

Similarly to Case Study 4, personal data obtained from the Electoral Roll should not be kept for longer than is necessary for the purpose for which it was originally obtained, i.e. for the purposes of public elections.

If a States Member used historical electoral data, then it is likely that they would breach the fifth principle, as they have clearly kept it for longer than was necessary to fulfil the purpose for which it was **originally** obtained, eg. the previous election campaign.

Note: In this scenario, the States Member may also breach the fourth principle as the accuracy of that data cannot be guaranteed.

6. Integrity and Confidentiality

Personal data must be processed in a manner that appropriately ensures its security, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

TOP TIPS

- Ensure appropriate security of all data you process, both electronic and paper based.
- This is more than just IT security – think access, use and disposal too.
- Look at your privacy policies – only you know how they stack up against reality!

Case Study 6:

A States Member holds a large amount of information on his home computer relating to constituents who are claiming welfare. The home computer is shared by his wife and their three teenage children. All the family use the computer on a daily basis and there are no password protected areas in the computer's hard drive. Essentially, the whole family have access to all areas of the computer, including the Parish welfare data.

One evening, the States Member's youngest son sends an e-mail to all his school friends, but instead of attaching a document containing an advert for the school magazine, he attaches the database containing details of all constituents claiming welfare.

In this example, the States Member as the data controller is responsible for ensuring the safeguard of the personal data held by him. This means that he must ensure that there are appropriate technical measures in place to safeguard that data, for example, password protection for those files containing this type of data.

In the case of an organisation holding personal data, which could be legitimately accessed by numerous members of staff, that organisation would also be expected to have appropriate organisational measures in place to safeguard the data, for example, robust policies and procedures governing the handling and processing of that data.

7. Accountability

Controllers are responsible for compliance with the data protection principles and must be able to demonstrate that compliance. More detailed guidance covering accountability can be

found here. Information relating to the duty to keep records, another part of accountability, can be found here.

TOP TIPS

- Work through each principle and document how you are taking steps to ensure compliance.
- Regularly review and update those documents

DATA SUBJECT RIGHTS

Personal data shall be processed in accordance with the rights of data subjects under this Law.

What this means:

All individuals have certain rights as provided in this Law. Those rights are detailed below and the relevant section of law is referenced should you wish to explore further.

States Members carry with them the same obligations as any other controller.

As such, all individuals who are the subjects of personal data held by a States Member have rights under the Law. Broadly, these are:

- Right to information at the point of collection (section 12 & 13);
- Right to data portability (section 14);
- Right of access to personal data held about them (section 15);
- Right to object to processing for direct marketing purposes (section 17);
- Right to object to processing on grounds of historical or scientific purposes (section 19);
- Right to rectification (section 20);
- Right to erasure (section 21);
- Right to restriction of processing (section 22);
- Right not to be subject to decisions based on automated processing (section 24);

Where a data subject exercises rights under the Law, the data controller is expected to comply with that request, unless an exemption under the Law can be claimed.

Case Study 7:

A States Member holds a database on their computer of all constituents. One of the constituents that did not vote for this States Member is unhappy that this politician is holding personal details about them and decides to submit a subject access request to that States Member to establish exactly what information is held by him.

The States Member upon receiving the request thinks of it as a nuisance and disposes of the letter in the nearest bin.

The Law requires that a controller, given sufficient information, must comply as soon as practicable and no later than one month.

BREACH REPORTING

The Law requires controllers to let the ODPA know when there has been a **personal data breach**.

A personal data breach is a breach of security leading to one or more of the following in respect of personal data-

- accidental or unlawful destruction
- loss
- alteration
- unauthorised disclosure
- unauthorised access

Personal data breach reports must be made to the ODPA using the online secure reporting form as soon as practicable and in any event no later than 72 hours after becoming aware of it.

In cases where a personal data breach is likely to pose a high risk to the significant interests of a data subject, controllers are also required to notify them of the breach.

August 2020