



Corporate Services Scrutiny Panel



Review into the Proposed Amendments to the Data Protection (Jersey) Law 2005

Presented to the States on the 19th April 2010

S.R.6/2010

CONTENTS

1.	CHAIRMAN’S FOREWORD	3
2.	TERMS OF REFERENCE AND PANEL MEMBERSHIP	4
2.1	TERMS OF REFERENCE	4
2.2	SUB-PANEL MEMBERSHIP	4
2.3	MAIN PANEL MEMBERSHIP	4
2.4	EXPERT ADVISOR	5
3.	KEY FINDINGS AND RECOMMENDATIONS	6
3.1	KEY FINDINGS	6
3.2	RECOMMENDATIONS	8
4.	INTRODUCTION	10
5.	BACKGROUND INFORMATION	12
5.1	DATA PROTECTION AND THE EUROPEAN UNION	13
5.2	DATA PROTECTION DIRECTIVE 95/46/EC	14
5.3	JERSEY AND THE EU	14
5.4	UNITED KINGDOM	15
5.5	IRELAND	16
5.6	GUERNSEY	16
5.7	HUMAN RIGHTS LEGAL OPINION	17
6.	AMENDMENT ONE	18
6.1	THE PROPOSAL	18
6.2	DEPARTMENTAL EFFECTS	21
6.3	THE POSITION IN THE UK	22
6.4	THE POSITION IN IRELAND	26
6.5	GUERNSEY	27
6.6	HUMAN RIGHTS	28
7.	AMENDMENT TWO	29
7.1	THE PROPOSAL	29
7.2	HUMAN RIGHTS	29
8.	AMENDMENT THREE	32
8.1	THE PROPOSAL	32
8.2	DEPARTMENTAL EFFECTS	36
8.3	THE POSITION IN THE UK	37
8.4	THE POSITION IN GUERNSEY	39
8.5	HUMAN RIGHTS	39
9.	AMENDMENT FOUR	41
9.1	THE PROPOSAL	41
9.2	DEPARTMENTAL EFFECTS	42
9.3	HUMAN RIGHTS	43
10.	AMENDMENT FIVE	44
10.1	THE PROPOSAL	44
10.2	DEPARTMENTAL EFFECTS	45
10.3	THE POSITION IN THE UK	47
10.4	THE POSITION IN IRELAND	47
10.5	HUMAN RIGHTS	49
11.	AMENDMENT SIX	50
11.1	THE PROPOSAL	50
11.2	HUMAN RIGHTS	50

12. AMENDMENT SEVEN.....	53
12.1 THE PROPOSAL.....	53
12.2 HUMAN RIGHTS.....	53
13. AMENDMENT EIGHT	54
13.1 THE PROPOSAL.....	54
13.2 DEPARTMENTAL EFFECTS.....	54
13.3 HUMAN RIGHTS.....	54
14. PUBLIC AWARENESS.....	55
15. CONCLUSION.....	58
16. APPENDIX 1 – THE PROPOSED DATA PROTECTON AMENDMENTS.....	59
17. APPENDIX 2 – EVIDENCE CONSIDERED.....	70
18. APPENDIX 3 – GLOSSARY OF TERMS	72
19. APPENDIX 4 – JONATHAN COOPER’S HUMAN RIGHTS LEGAL OPINION.....	73
20. APPENDIX 5 – ADVOCATE HELEN RUELLE’S REPORT	84
21. APPENDIX 6 – MINISTER FOR ECONOMIC DEVELOPMENT: LETTER 23RD MARCH 2010	95
22. APPENDIX 7 – MINISTER FOR ECONOMIC DEVELOPMENT: LETTER 3RD MARCH 2010	96

1. CHAIRMAN'S FOREWORD

As time goes by, Governments around the world are consistently producing new legislation and amending existing legislation to adapt to the movement of modern day globalisation and particularly the changes surrounding European Union Directives.

Data Protection can be seen as a complex law which is usually incorporated into many areas of legislation throughout various jurisdictions. This legislation is in place to promote and establish common sense amongst all individuals and businesses alike, as many people will be aware personal details are very much that – personal!

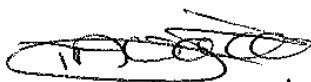
Awareness is a key component of data protection whereby we should all be able to comprehend that if we were to expose a person's personal details without their consent this could impose serious consequences or implications for that person therefore, this could be life changing not only for them but for their family as well.

Taking all these factors into account the Sub-Panel felt it only appropriate to ensure that such changes to legislation were appropriate for the Island in response that it would not cause unnecessary bureaucracy and further misunderstanding of the application of the law.

It has been a belief that Data Protection was introduced to place a responsibility upon an entity, this being a business, which in particular areas can store hundreds of thousands of people's personal details at a touch of a button, especially this day in age.

Unfortunately the Sub-Panel had a tight timeframe in order to complete this report therefore, purely focussed on the draft amendments in relation to data protection. I would like to take this opportunity to thank all Members of the Sub-Panel for their hard work, availability and dedication to this task.

I would also like to thank our advisor Advocate Helen Ruelle for her expertise and legal advice on these matters, it has been very much appreciated.



Deputy T. Vallois
Chairman
Corporate Services Data Protection Sub-Panel

2. TERMS OF REFERENCE AND PANEL MEMBERSHIP

2.1 TERMS OF REFERENCE

The following Terms of Reference were established for the Data Protection review:

1. To review the proposed amendments of the Law with particular regard to:
 - a. The implications surrounding the proposed amendments;
 - b. The language and robustness;
 - c. A comparison with other jurisdictions, namely the United Kingdom and Ireland.
2. To consider whether the proposed amendments are in the interest to whom the law applies, and whether there are any manpower or financial implications.
3. To consider whether the proposed amendments comply with the Human Rights (Jersey) Law 2000.
4. To examine any further issues relating to the topic that may arise in the course of the Scrutiny Review and which the Panel considers relevant.

2.2 SUB-PANEL MEMBERSHIP

For the purposes of this review, the Corporate Services Scrutiny Panel established the following Sub-Panel:

DEPUTY T.A. VALLOIS, CHAIRMAN
DEPUTY D.J. DE SOUSA, VICE-CHAIRMAN
SENATOR S.C. FERGUSON
DEPUTY M.R. HIGGINS

2.3 MAIN PANEL MEMBERSHIP

The Corporate Services Scrutiny Panel itself comprises of the following members:

SENATOR S.C. FERGUSON, CHAIRMAN
DEPUTY C.H. EGRE, VICE-CHAIRMAN
CONNETABLE D.J. MURPHY
DEPUTY T.A. VALLOIS

2.4 EXPERT ADVISOR

The Corporate Services Panel appointed the following expert advisor:

Advocate Helen Ruelle of Mourant du Feu & Jeune

Mrs Ruelle trained and qualified as an English solicitor in 1998 (currently non-practising) and has worked in both private practice and as a senior in-house lawyer for a UK public sector body before joining Mourant du Feu & Jeune in 2001. Mrs Ruelle was sworn in as a Jersey advocate in 2008. Advocate Ruelle specialises in commercial and corporate issues relating to Jersey companies, employment, data protection and competition law.

3. KEY FINDINGS AND RECOMMENDATIONS

3.1 KEY FINDINGS

- 3.1.1 The wording of proposed amendment one causes concern to the Sub-Panel in its current context.
- 3.1.2 The Sub-Panel acknowledges that a person can appeal against an information notice however, is concerned that not everyone is aware of data protection. If the Commissioner has an increased power in its current format to issue anyone with a notice, the public need to be aware that there is an appeal process.
- 3.1.3 The Sub-Panel is concerned that costs would become apparent in Jersey, although on a lesser scale, and these concerns are enhanced further after learning that the Commissioner's Office consists of a very small team, particularly with the possibility of extending her remit.
- 3.1.4 The Sub-Panel acknowledges Guernsey's decision in adopting an amendment which increases the Commissioner's information notice power because it has been focussed in one particular area - *The European Communities (implementation of Council Directive on Privacy and Electronic Communications) (Guernsey) Ordinance*.
- 3.1.5 The Sub-Panel acknowledges that the UK Act applies the seven years required experience and accepts that by removing it from the Data Protection (Jersey) Law 2005, could affect confidence levels in the Tribunal.
- 3.1.6 The Sub-Panel is interested to note that there appears to be a discrepancy between Articles 60 and 55. A person may be liable to 2 years imprisonment under Article 55, but a person may also be liable to 5 years imprisonment under Article 60. Article 55 relates directly to an information notice whilst Article 60 may also potentially relate to an information notice.
- 3.1.7 In comparison to the UK, the Sub-Panel has found that a "reasonable belief" Public interest test has not been added to the Data Protection (Jersey) Law 2005 under Article 55, to protect journalistic activity.

- 3.1.8 Evidence suggests that increasing the penalty to two years imprisonment for unlawful obtaining would act as a deterrent. It was also noted that penalties of imprisonment are incorporated into other Jersey legislation for Data Protection breaches.
- 3.1.9 The Sub-Panel found a potential loophole regarding the amendment to include equipment found on premises, rather than 'other material' and Article 61 of the Data Protection (Jersey) Law 2005 which refers to any documents and other material.
- 3.1.10 The Sub-Panel noted the inequity between Health and Social Services and other businesses for subject access requests. It was also noted that Jersey should follow the EU Data Protection Directive 95/46EC which states that data should be supplied without excessive expense. During the transitional period when the fee was a maximum of £50 the Health Department used their discretion, on what seemed to the Sub-Panel, a fair basis.
- 3.1.11 The Sub-Panel accepts that there may be an issue of inequality between charities being exempt from the notification fee, and small businesses.
- 3.1.12 Evidence from the Public Hearings suggested that there is a low level of awareness of Data Protection.

3.2 RECOMMENDATIONS

- 3.2.1 The Sub-Panel would strongly recommend that the Commissioner reconsiders the wording and format of the draft legislation for amendment one as it currently stands.
- 3.2.2 The Sub-Panel recommends that the public are made more aware of the Data Protection Tribunal, and that it is more accessible to the public if an increase in power is to be adopted.
- 3.2.3 The Sub-Panel suggest additional research is carried out into the manpower and financial costs of the proposed amendments, which has been conducted in the UK.
- 3.2.4 The Sub-Panel recommends that Jersey explores the possibility of adopting a Privacy and Electronic Communication Regulation.
- 3.2.5 The Sub-Panel recommends that the seven years required experience for the President of the Tribunal should remain however, a degree of discretion should be allowed. It also suggests that the Law should provide, in addition to discretion, that whilst the person must be a locally qualified lawyer, the seven years' experience need not be as a locally qualified lawyer.
- 3.2.6 The Sub-Panel recommend that penalties for all breaches are clarified before an amendment to increase the maximum penalty for offences under Article 55 is lodged.
- 3.2.7 It is strongly recommended that Jersey should follow the UK precedent by adding a "reasonable belief" public interest test to Article 55 of the Law.
- 3.2.8 The Sub-Panel recommend that there should be a public awareness campaign to address changes in the Data Protection Law. This could be beneficial because it could work in favour of the deterrence factor carried with some of the amendments.
- 3.2.9 The Sub-Panel recommend that the word "equipment" is included in Article 61 to avoid any potential discrepancies in a Court of Law. Furthermore, it recommends that the Law should be revisited to ensure there are no other incidences of potential loopholes.

- 3.2.10 The Sub-Panel suggests that the maximum fee of £50 for subject access requests should be charged across the board. It further suggests that this should remain on a discretionary basis.
- 3.2.11 The Sub-Panel considers charities being exempt from the notification fee as acceptable, however recommends that this is reviewed in the context of small businesses.
- 3.2.12 The Panel recommends that if the amendments were to be adopted, in particular amendment one, the general public and businesses need to be fully aware so that they can comply with the Law.

4. INTRODUCTION

For the purposes of this report:

- Jersey: The Data Protection (Jersey) Law 2005 shall be known as “the Law”
- Ireland: The Data Protection 1988 Act and Data Protection (Amendment) Act 2003 shall be known as the “Ireland” Acts
- UK: The Data Protection Act 1998 shall be known as the “UK” Act
- Guernsey: Data Protection (Bailiwick of Guernsey) Law 2001 as amended shall be known as the “Guernsey” Law.

Globalisation is no longer just a word it is reality – in economic, technological, and social terms. Data Protection is fundamental in the global context. Regulating the privacy of personal information and safeguarding that information is pivotal for governments everywhere. The amendments have been explored to investigate whether they would heighten the Law and make the data protection regime more robust.

On 16th September 2009, the Minister for Treasury and Resources lodged an amendment to the Data Protection (Jersey) Law 2005 (P.147/2009). The amendment called to provide the Commissioner with powers to serve information notices on other relevant persons in addition to data controllers and processors. It also called for the removal of the requirement for the Tribunal President to have seven years’ experience standing as an advocate or solicitor.

The Corporate Services Scrutiny Panel took an interest in the amendment and identified that further amendments were to be lodged. The Sub-Panel found it interesting that P.147/2009 stated *“that in light of local experience as well as changes made to U.K. legislation, the following amendments to the Data Protection (Jersey) Law 2005 are proposed”*. This was somewhat ambiguous because the UK has not brought an increased power in this format. The UK has yet to adopt data processors within its Law.

The Minister for Treasury and Resources agreed to withdraw P.147/2009 to enable the Panel to review all the proposed amendments. A Sub-Panel was formed to carry out this review. The amendments have not yet been lodged by the Minister for Treasury and Resources.

In brief, the proposed amendments to the Law are as follows:

1. **Amending the provisions in relation to information notices;** if this amendment was adopted, the Commissioner would have an increase in power to serve an information notice on a person other than a relevant data controller or data processor.
2. **Amending the professional requirements in relation to the President of the Data Protection Tribunal;** if this amendment was adopted, the President of the Data Protection Tribunal would not be required to be of seven years standing as an advocate or solicitor.
3. **Amending the maximum penalty applicable to an offence under Article 55 of the Data Protection (Jersey) Law 2005;** if this amendment was adopted, the maximum penalty would be increased to two years imprisonment and/or a fine.
4. **Amending the power of seizure to include equipment found on premises;** if this amendment was adopted, equipment as well as documents and “other material”, could be seized under a warrant.
5. **Amending the maximum fee chargeable for subject access requests relating to health records;** if this amendment was adopted, it would allow data controllers (who are required to respond to subject access requests relating to personal data defined as a health record) to charge a maximum of £50.
6. **Amending the provisions relating to subject access exemptions for trustees;** if this amendment was adopted, it would allow restrictions on information provision relating to trustees (contained within the Foundation (Jersey) Law 2009) to be recognised within the Law.
7. **Amending the provisions relating to subject access exemptions;** if this amendment was adopted, it would add Article 41 of the Drug Trafficking Offences (Jersey) Law 1998 to the list of miscellaneous exemption contained within the Data Protection (Subject Access Exemptions) (Jersey) Regulations 2005.
8. **Amending the provisions relating to the notification fee from charities;** if this amendment was adopted, it would allow data controllers whose sole processing activities relate to charity work to be exempt from the notification fee.

5. BACKGROUND INFORMATION

The main focus of the review are the proposed amendments to the Law, which came into force on 1st December 2005, bringing Jersey into line with European legislation. There are 8 Data Protection Principles¹ which set enforceable standards for the collection and use of personal data:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained for only one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or purposes;
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4. Personal data shall be accurate and, where necessary, kept up to date;
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under this Law;
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area 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.

The Law has been in force for five years and 2008 saw the end of the “transitional period”. The transitional period allowed organisations an opportunity to incorporate the substantial new legal requirements contained within the Law into their processes².

¹ The Office of the Data Protection Commissioner, Annual Report 2008, P.1

² The Office of the Data Protection Commissioner, Annual Report 2008, p.4

The Sub-Panel has studied the proposed amendments and during the review it became apparent that amendments one and three could be the most controversial, out of the eight amendments.

During the Public Hearing with the Data Protection Commissioner, the Sub-Panel asked for the reasoning behind each amendment. It identified that the proposed amendments are not retrospective:

“There is no retrospective-ness about it. I base it on my own experience. I base it on discussions with other regulators. The pressure from my ... there is no other agenda other than local legislations looking to us for remedy and the increase in the amount of data going through Jersey companies, especially fulfilment type companies where you have very, very large databases. That is the basis of this. These have been in train for a couple of years now, I think, to put a bit of perspective on it³.”

During the review the Sub-Panel felt it was important to research other jurisdictions to explore whether they have already adopted the same amendments that Jersey is proposing. Some of the jurisdictions considered, namely Ireland and the UK, are part of the European Union; therefore the European Union and Data Protection which applies to them must be explained.

5.1 DATA PROTECTION AND THE EUROPEAN UNION

The advance of computer technology is allowing personal data to travel across borders more easily than ever before. As a result, data relating to citizens of one Member State are sometimes processed in other Member States of the European Union. Consequently, because data is collected and exchanged more frequently, regulation on data transfers becomes necessary⁴.

National laws regarding data protection demand good data management from bodies that process data, namely data controllers. There is an obligation to process data fairly and in a secure manner and to use personal data only for explicit and legitimate purposes⁵. National laws also guarantee a series of rights for individuals, such as:

³ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.15

⁴ Data Protection in the European Union, European Commission Office UK, p.3

⁵ Data Protection in the European Union, European Commission Office UK, p.3

- The right to be informed when personal data was processed and the reason for this processing;
- The right to access the data and if necessary;
- The right to have the data amended or deleted.

In the past, national laws on data protection aimed to guarantee the same rights, although some differences existed. These differences could create potential obstacles to the free flow of information⁶.

For these reasons, there was a need for action at European level, and this took the form of EC Directives.

5.2 DATA PROTECTION DIRECTIVE 95/46/EC

The Data Protection Directive (officially known as the Directive 95/46/EC) on the protection of individuals with regard to processing of personal data and on the free movement of such data is a European Union directive. The Directive regulates the processing of personal data within the European Union. It is important to note that it is a fundamental component of EU privacy and human rights law. The directive was implemented in 1995 by the European Commission⁷.

The data protection rules apply not only when responsible parties (called the controller in this EU directive) is established or operates within the EU, but whenever the controller uses equipment located inside the EU to process personal data. Therefore, controllers from outside the EU who process personal data inside the EU must comply with this directive. EU Member States set up supervisory authorities whose job is to monitor data protection levels in that State, and to advise the government about related rules and regulations, and to initiate legal proceedings when data protection regulations are broken⁸.

5.3 JERSEY AND THE EU

The Sub-Panel recognises that Jersey is not part of the EU, however, feels it is important to note that the Law is based on the UK Act. The UK is a member of the EU and therefore complies with EU Directives. The UK Act was brought into force to comply with the relevant EU Directive. The Law was brought into force to bring Jersey in line with other European jurisdictions and to achieve “adequacy”.

⁶ Data Protection in the European Union, European Commission Office UK, p.3

⁷ European Parliament Report to the Implementation of the Data Protection Directive 95/46/EC p.13

⁸ European Parliament Report to the Implementation of the Data Protection Directive 95/46/EC p.13

5.4 UNITED KINGDOM

The UK Act came into force in 1998. It establishes a framework of rights and duties which are designed to safeguard personal data. The framework aims to balance the legitimate needs of organisations to collect and use personal data for business and other purposes against the rights of an individual in respecting the privacy of their personal details. The legislation is underpinned by a set of eight principles⁹, which are very much the same as Jersey's.

1. Personal data shall be processed fairly and lawfully and in particular shall not be processed unless –
 - a. At least one of the conditions in Schedule 2 is met; and
 - b. In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

⁹ "The Guide to Data Protection" (2009) Information Commissioners Office, p.40

8. Personal data shall not be transferred to country or territory outside the European Economic Area 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.

The UK's equivalent to Jersey's Data Protection Commissioner is the "Information Commissioner". The Information Commissioner is the UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner has responsibilities in respect of freedom of information as well as data protection¹⁰.

5.5 IRELAND

The main Irish law dealing with data protection is the Data Protection Act 1988. The 1988 Act was amended by the Data Protection (Amendment) Act 2003. The 2003 Act brought the Law in line with the EU Data Protection Directive 95/46/EC.

5.6 GUERNSEY

The Guernsey Law came into force in 2001. The Law is intended to bring the level of protection within the Bailiwick up to an adequate standard. The statutory instruments giving effect to the Law were made by the Advisory and Finance Committee in July 2002 and were laid before the States, enabling the Law to come into force on 1st August 2002. Subsequent secondary legislation had been made in 2002, and further amendments to the Guernsey Law came into force on the 1st March 2010.

The Guernsey amendments include:

- Amendment to increase the notification fee from £35.00 to £50.00;
- Amendment to insert a new section "Exclusion of Liability";
- Amendment to ensure a person guilty of an offence under section 55 is liable on summary conviction (Magistrates), to imprisonment for a term not exceeding 12 months, and a conviction on indictment (Royal Court), to imprisonment for a term not exceeding 2 years or to a fine, or both.

¹⁰ The Guide to Data Protection" (2009) Information Commissioners Office, p. 11

5.7 HUMAN RIGHTS LEGAL OPINION

The Human Rights (Jersey) Law 2000 was adopted by the States in February 2000 and came into force in December 2006. The Sub-Panel sought a legal opinion¹¹ from Mr J. Cooper of Doughty Street Chambers, London on the following issues:

- What human rights issues are raised by, in particular, amendment one, which increases the Commissioner's power to issue an information notice on a person other than a data controller or data processor?
- Taking into account the issues, is the situation human rights compliant?
- Should it be advised that the amendments are not human rights compliant, what recommendations for changes would render them compatible?

Mr Cooper explained that he expresses particular concern in relation to amendments two and six:

The amendments of particular concern in the above list relate to the professional requirements of the Tribunal President and the effective exemption of Foundations from the scope of the Data Protection (Jersey) Law. Both of these potentially raise serious human rights concerns, whereby the amendment itself (if passed into law) could be found in breach of the Human Rights (Jersey) Law 2000. Consequently, there are doubts that these amendments, as currently formulated, could be given a statement of compatibility under Article 16 of that Law.

Full analyses of Mr Cooper's opinions are explained after each section of the amendments. The Sub-Panel has not had the opportunity to receive comments from the Law Officers Department on Mr Cooper's legal opinion.

The draft legislation for the proposed Jersey amendments can be found in appendix one.

¹¹ Mr Cooper's advice is available to read in appendix 4

6. AMENDMENT ONE

6.1 THE PROPOSAL

Amending the provisions in relation to information notices; if this amendment was adopted, the Commissioner would have an increase in power to serve an information notice on a person other than a relevant data controller or data processor.

The Law, in its current form only enables the Commissioner to serve an information notice on a data controller and a data processor only. During the Public Hearing, the Commissioner outlined two cases where an individual, in possession of the required information, had been willing to divulge the information, even though they were not a data controller or processor. Although there had also been two occasions where the individual, in possession of the required information, had been unwilling to divulge the required information. The Commissioner said:

“.....there have been a couple of occasions, and they have been very serious occasions, where the individual has just said: “No, we are not going to assist.” It poses a very huge problem for us, because if we do not know where the source of the security breach, for example, is we cannot investigate it, so we have had to walk away on a couple of occasions¹².”

The Sub-Panel notes that the Commissioner referred to “a couple of occasions” whereby she was unable to acquire information. Considerable concern was expressed with this amendment as the Sub-Panel felt that Jersey may possibly be over legislating for something that occurs infrequently. Even if an individual is not willing to divulge the source of the information, police assistance can be sought by the Commissioner in certain circumstances:

“On a couple of other occasions we have sought police assistance to further investigate under Article 55 to require that person to provide us with evidence under caution. On those occasions where the police have become involved I still remain slightly uncomfortable that it seems to be a bit of a leap that if we could obtain the information through the regulatory route it would be preferable. It would be less, I have used the word: “heavy handed” in the report and that really to sum it up is how I feel¹³.”

¹² Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.13

¹³ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.3

“PLUGGING THE GAP”

The Commissioner considers there to be a gap in the current Law:

“We are not handing the investigation over to the police, but we are asking for police assistance under our law. So the power is in the law now but there seems to be a gap as everything else seems to be reasonable steps. At each point you can take the next step to move it up a notch. There seems to be a step missing here that either the investigation falls away because you have not been able to get the information off the person or you bump it up to a criminal¹⁴.”

In circumstances where an individual has not agreed to provide information voluntarily and where there are no grounds for a police investigation pursuant to Article 55, the Commissioner has had to cease an investigation where it is believed that there is still a potential breach to be investigated. The Commissioner's view is that there is therefore a gap in the powers available.

It is also the Commissioner's view that in some circumstances dealing with a matter under Article 55 is "heavy handed" and that matters could be better dealt with under the regulatory powers which are sought by amendment one.

Although a balance needs to be identified between the regulatory and the criminal sanction of the Law, the Sub-Panel is somewhat apprehensive that an information notice could be served on an individual such as a neighbour:

“If information about you, if your neighbour comes up to you today and says: “Oh, I hear X, Y, Z about you” and you think: “Well, only 5 people know that and I have kept that information secure” and you complain to us that that information somehow has leaked out from one of those 5 organisations, think about your medical records or a job application or anything that you want to keep private and we say to you: “Sorry” because we cannot approach your neighbour and ask them where they got it from. We do not want to treat neighbours as criminals, we just need them to provide us the information so that we can look to the source. If somebody has left your application form or your medical records somewhere, somebody has not looked after that data properly then we need to know about it and very rarely that route is only available to us via an individual as opposed to an organisation¹⁵.”

¹⁴ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.4

¹⁵ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.6

However, extending the Commissioner's power may help to prevent an individual, such as a neighbour, from being treated as a criminal and ensure the Commissioner is able to approach the role in a more regulatory manner. It has to be noted that an individual could still be party to criminal action if they do not comply with the information notice that is served upon them. Bearing this in mind, by introducing a wider power such as this, could cause confusion and complications in an already complicated piece of legislation.

KEY FINDING

The wording of proposed amendment one causes concern to the Sub-Panel in its current context.

RECOMMENDATION

The Sub-Panel would strongly recommend that the Commissioner reconsiders the wording and format of the draft legislation for amendment one as it currently stands.

The Legislation currently sets the onus on the data controller to ensure that any personal information processed within their organisation is kept secure, from the current Commissioner's perspective this will still be the case. The amendment looks to obtain information from an individual in order to identify the data controller who has possibly breached the law:

“What you are trying to do is to establish which data controller it is that has got the problem. Your flow stops there and really once the information is given to us if the information ... we have had a case where a file was left on the top of a bin in King Street and the person that found it, we do not have any beef with them at all. We need to know where they found it, which office was it near so that we can start looking at where ... there was highly sensitive information in that file and as I say that person walked into our office and said: “Look what I have just found” and we looked at it horrified. We had a number of people, it would have to go to about half a dozen people now but if that person had said: “I saw that office worker dump it on that bin” we need to know that. So as to the individual I see what you are saying about the sanction and ultimately if you are serious about a law you have to say: “Listen, what we say goes or there is a sanction” but we need to find the source of that problem, so you are focusing on the data controller. We are not looking at individuals and saying you have got a whole regulatory regime to deal with. They have got their domestic use exemption. That all applies. It is just about when and if one individual comes to us

and feels that they have had their rights infringed under this law it is how we get to the source of the problem. So I do think it is proportional, I do think it is reasonable¹⁶.”

This in turn heightened the interest of the Sub-Panel as to the checks and balances that will be in place to ensure the power could not be used unnecessarily. The draft legislation as currently formatted would require the Commissioner, when serving an information notice, to explain her reasoning for doing so, at which point if the person of which the information notice has been served upon does not believe this is appropriate, they can call upon the Data Protection Tribunal to appeal against the notice.

KEY FINDING

The Sub-Panel acknowledges that a person can appeal against an information notice however, is concerned that not everyone is aware of data protection. If the Commissioner has an increased power in its current format to issue anyone with a notice, the public need to be aware that there is an appeal process.

RECOMMENDATION

The Sub-Panel recommends that the public are made more aware of the Data Protection Tribunal, and that it is more accessible to the public if an increase in power is to be adopted.

6.2 DEPARTMENTAL EFFECTS

The views from the States of Jersey Police were sought, in relation to the effect on police workload of amendment one, if it was adopted. The Sub-Panel found it interesting that cases relating to this amendment were not common:

“The number of cases specific to this amendment are few and far between. It is anticipated that some benefit may result in terms of potential reduction in Police workload due to introduction of this amendment. This is due to the fact that at present, where the Commissioner has ‘narrower’ powers to serve and information notice, then the Commissioner is reliant on a need to seek police assistance to progress the matter by use of specific police powers¹⁷.”

¹⁶ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.6

¹⁷ Letter from States of Jersey Police, 18th February 2010

6.3 THE POSITION IN THE UK

The Information Commissioner in the UK has been pressing for the same increase in power. Currently the Information Commissioner's information notice power under the UK Act only enables him to require information from the data controller, whereas the Commissioner in Jersey already has the power to serve an information notice on both a data controller and a data processor. The Information Commissioner has some information gathering powers under the Regulation of Investigating Powers Act, but these can only be used in the investigation of criminal offences. These are circumstances where he needs to obtain information from someone other than the data controller in order to investigate non-criminal data protection breaches. This happens most commonly in relation to breaches of the Privacy and Electronic Communications Regulations 2003 (PECR), where it may be necessary to identify for example, who the subscriber to a particular phone or fax number is, or who is 'behind' an e-mail address or website¹⁸.

The Sub-Panel sought the views of the Deputy Information Commissioner in the UK. Regarding this matter, he stated in an email to the Sub-Panel:

“The most pressing reason why we have argued for such a power is to enable the investigation of breaches of the Privacy and Electronic Communications Regulations 2003. When an unsolicited phone call, fax or email is received it is not always clear to the recipient who the originator of the message is. It is this originator who will be the relevant data controller on whom the regulations bite. They therefore need to be identified by the Commissioner. Typically it is the provider of the relevant telecommunications service who holds the information necessary to identify who the subscriber to a particular phone number is, or who is “behind” an email address or website. Without access to such information it can prove impossible for the Commissioner to either identify the sender of an offending message or tie an offending message evidentially to a particular sender. The Commissioner therefore needs the power to serve an information notice on a telecommunications service provider and not just on a data controller.”

The Sub-Panel found it interesting that the case put forward by the Information Commissioner appears to have been based predominately but not exclusively on the need to address concerns in relation to investigations concerning PECR. This was also a concern of the Minister for Economic Development, who raised the issue in his letter dated 3rd March (appendix 7):

¹⁸ Data Protection Powers and Penalties, The Case for Amending the Data Protection Act 1998, p.10

“Although the Commissioner’s Report states that difficulties have been encountered in obtaining information in the course of investigations, no details are provided and I am not aware that PECR breaches are of particular concern in Jersey. I would therefore question the need for the Commissioner to have the extended powers that were requested, but ultimately not granted, in the United Kingdom¹⁹.”

The Deputy Information Commissioner also mentioned that they have been pressing for an increase in power in order to help:

- make the initial identification of the relevant data controller, assisting our investigation of cases where a number of organisations are involved in a complex data processing operation;
- obtain evidence of a data controller’s breach from someone other than the data controller themselves;
- investigate the processing of personal data carried out on behalf of a data controller by a data processor;
- obtain further information where a security breach by a data processor may be causing problems for a number of data controllers that it provides services for, whose identity we may not know and who may themselves be unaware of the problem.

CORONERS AND JUSTICE ACT 2009 IN UK

The Coroners and Justice Act 2009 received Royal Assent on 12 November 2009 and in comparison to Jersey’s amendment one, included measures to:

- amend the UK Act to strengthen the Information Commissioner's inspection powers

In an impact assessment (*enhancing the inspection powers of the Information Commissioner*), the Ministry of Justice published a paper in January 2009 to summarise the invention and options in amending the UK Act for the Information Commissioner to have enhanced powers when issuing inspection powers.

¹⁹ Letter from Minister for Economic Development, 3rd March 2010

Enhancing the inspection powers of the Information Commissioner would ensure, according to the Ministry of Justice, that the Information Commissioner has access to the information he requires to effectively carry out his duties, particularly when the Information Commissioner suspects a data controller is trying to evade investigation.

The paper also outlined the cost of promoting good practice and encouraging data controllers to come forward for advice, and enforcing compliance and enhancing the inspection powers of the Information Commissioner:

Figure 1: Impact Assessment Enhancing the inspection powers of the Information Commissioner

Summary: Analysis & Evidence			
Policy Option: 3 & 4	Description: Promoting good practice and encouraging data controllers to come forward for advice Enforcing compliance and enhancing the inspection powers of the Information Commissioner		
COSTS	ANNUAL COSTS	Description and scale of key monetised costs by 'main affected groups' The costs incurred by the ICO as a result of additional work will be met by a new funding structure (see consultation document . http://www.justice.gov.uk/docs/cp1508.pdf) Minimal costs will be incurred by the courts from an increase in the application for Schedule 9 warrants.	
	One-off (Transition)		Yrs
	£ 2,500,000		1
	Average Annual Cost (excluding one-off)		
	£ 6,000,000	Total Cost (PV) £	
Other key non-monetised costs by 'main affected groups' The costs noted above are not in addition to those noted in the impact assessment on ICO funding (see consultation document). Additional funds raised by the proposal on ICO funding are required to cover the cost of the functions covered in this impact assessment.			

It found that there would be significant costs to the Information Commissioner's Office. The Ministry of Justice is currently looking into the funding arrangements of the Information Commissioner's Office for his increased data protection work.

The Sub-Panel is aware that this does not relate specifically to amendment one and would not incur the costs as quoted above, however it does demonstrate that thorough research has been carried out in the UK. The Sub-Panel would expect there to be some costs to the Commission, but this would be significantly lower for a small jurisdiction such as Jersey. The Commission maintains that no such costs are envisaged with the proposed amendments. The Sub-Panel is concerned that this has not been explored fully as it has been within the UK. The Commissioner in Jersey mentioned that she is working with a very small team which consists of herself, a Deputy Commissioner and two administrative support staff:

“I am fiercely tight when it comes to money and I am fiercely protective of what is a very effective team with very limited resources and a very wide remit. There are huge advantages to having a small team but what I have found is when I first started in this job it was a very proactive task I had to educate, get out there and talk about the message, especially when the law was coming in. In a sense, I am sort of reaping the rewards of that now because ... also it is a change in climate generally, but people are much more willing to come forward and complain. The one thing that does concern me, for the record, is our capacity for dealing with complaints. We are struggling²⁰.”

KEY FINDING

The Sub-Panel is concerned that costs would become apparent in Jersey, although on a lesser scale, and these concerns are enhanced further after learning that the Commissioner’s Office consists of a very small team, particularly with the possibility of extending her remit.

RECOMMENDATION

The Sub-Panel suggest additional research is carried out into the manpower and financial costs of the proposed amendments.

FREEDOM OF INFORMATION CAMPAIGN

The Sub-Panel sought the views of Mr Maurice Frankel, Director for the Campaign for Freedom of Information in the UK. Mr Frankel asks whether this amendment might allow information about journalists’ sources to be obtained without following the Law’s existing safeguards for journalism.

Mr Frankel explained that currently, media organisations have special protection from the data protection provisions because Article 10 of the European Convention on Human Rights which recognises the need to protect freedom of expression.

Pursuant to the Law, personal data which are processed only for the purposes of journalism are exempt from, most notably in these circumstances, a data subject access request if:

- the processing is undertaken with a view to the publication by any person of journalistic material; and

²⁰ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.29

- the data controller reasonably believes publication would be in the public interest having regard to the special importance of the public interest in freedom of expression; and
- the data controller reasonably believes that in all the circumstances, compliance with the relevant provisions of the Law is incompatible with the purposes of journalism.

Mr Frankel queries whether it may be possible that the enhanced power to serve information notices might allow a notice to be served on someone suspected of being a journalist's *source*, requiring the individual to provide information confirming that he or she is the source. He goes on to state:

“At present, no information notice could be served on such individuals. There may also be other implication for media reporting, or the uncovering of wrongdoing. The result might be to permit an interference with freedom of expression of a kind which the existing Law seeks to restrict.”

The Sub-Panel acknowledges Mr Frankel's point that even with the current safeguards around “special purposes” additional safeguards have been introduced in the UK.

6.4 THE POSITION IN IRELAND

In contrast to the UK and Jersey, the Ireland Act already allows the Commissioner to issue an information notice on any other person.

The Sub-Panel was provided with written submission from the Deputy Commissioner in Ireland explaining that an information notice had not been issued and the amendment was brought in because it would be ‘useful’ to have the ability to issue a notice to any other person:

“...the Commissioner has not served an information notice on any entity that is neither a data controller or a data processor but certainly as we see more individuals send unsolicited emails etc it would seem that having an ability to serve an information notice in such circumstances is useful.”

The Sub-Panel understand that if this amendment is adopted it may not be used frequently, if at all, and would not necessarily mean it would not be a desirable aspect of the Law.

However noting the Sub-Panel's earlier comments relating to serving an information notice on an individual such as a neighbour it should be duly noted that the Deputy Commissioner provides an example with regards to electronic communication.

6.5 GUERNSEY

The Sub-Panel found it interesting to note that Guernsey had adopted *The European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Guernsey) Ordinance*, in 2004. The Ordinance states:

“The purpose of this Ordinance is to implement in respect of the Islands certain provisions concerning the processing of personal data and the protection of privacy in the electronic communications sector as referred to in the Directive, with the intent that standards of protection within the Islands meet or are consistent with the standards provided for by the Directive [2002/58/EC on privacy in the electronic communications sector].”

As explained in section 6.3, the UK Information Commissioner has put forward his case for extended power in issuing information notices to any person primarily, but not exclusively, because of the need to address concerns in relation to investigations concerning privacy and electronic communications breaches.

This Ordinance has been amended into the Guernsey Law to allow the service of an information notice on any relevant person, with effect from 1st March 2010. These Regulations accord closely with those which came into force in the UK at the end of 2003.

The Sub-Panel found it interesting to note that no such regulations concerning Privacy and Electronic Communications have been adopted in Jersey. It is also worth pointing out that Guernsey has enacted the Ordinance into its Law, consequently focussing it into privacy and electronic communications breaches. Jersey draft legislation on the other hand, allows a notice to be issued to any person, not relating it specifically to privacy and electronic communication breaches. Therefore, the Sub-Panel questions the need for amendment one.

The Sub-Panel's advisor, Advocate Ruelle, also makes a point in her report²¹, in relation the PECR Regulations and Guernsey:

²¹ Advocate Helen Ruelle's full report can be read in appendix 5

It is understood that the Data Protection (Bailiwick of Guernsey) (Amendment) Ordinance 2010 (the "Amendment Ordinance") amends the Guernsey Law. The Amendment Ordinance appears, in summary, to extend the Guernsey Commissioner's powers to serve information notices, in certain circumstances, on data processors in addition to data controllers. Prior to the coming into force of the Amendment Ordinance, it is understood that the Guernsey Commissioner was only able to serve an information notice on a data controller.

[The] Guernsey law has been amended to allow the service of information notices concerned with alleged breaches of electronic communications regulations on any person (although the author of this report has been unable to locate the amending provision to the Guernsey Law which effects this).

Therefore, it appears that in Guernsey, the power to serve information notices on any person only extends to alleged breaches of the electronic communications regulations, which the author takes to mean the Ordinance or subordinate legislation thereunder.

KEY FINDING

The Sub-Panel acknowledges Guernsey's decision in adopting an amendment which increases the Commissioner's information notice power because it has been focussed in one particular area - *The European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Guernsey) Ordinance 2004*.

RECOMMENDATION

The Sub-Panel recommends that Jersey explores the possibility of adopting a Privacy and Electronic Communication Regulation.

6.6 HUMAN RIGHTS

Mr. Cooper of Doughty Street Chambers and a human rights expert welcomes this amendment to the Law. He believes that Article 43 as amended, and coupled with existing safeguards built into the Law, which guarantee the right to appeal, and the suspension of the process whilst the appeal is pending, as well as the duty to make a statement explaining why the information notice is being served, will enhance the data protection regime in Jersey²².

²² Mr Cooper's legal opinion can be found in appendix 4

7. AMENDMENT TWO

7.1 THE PROPOSAL

Amending the professional requirements in relation to the President of the Data Protection Tribunal; if this amendment was adopted, the President of the Data Protection Tribunal would not be required to be of seven years standing as an advocate or solicitor.

According to the Commissioner, amending the professional requirement of the President of the Data Protection Tribunal would “*widen the pool of people that we have to choose from*”²³. Data Protection is a specialised area, and by removing the requirement for the President to be of seven years standing as an advocate or solicitor would allow more people to choose from.

7.2 HUMAN RIGHTS

Initially the Sub-Panel was of the view that this amendment is not controversial, and therefore accepted the reasoning behind it. However, the legal opinion sought from Mr J. Cooper suggests that this amendment could undermine confidence in the Tribunal.

Mr Cooper goes on to state that the Data Protection Tribunal, by definition, would be dealing with matters of law and fact of significant complexity. He believes that if proposed amendment one is accepted, that complexity will be increased. Therefore, the President of the Tribunal has to have sufficient standing, as well as its appearance, to be able to manage these issues and inspire confidence in all concerned. Mr Cooper considers removing the professional requirement qualification of seven years standing could undermine confidence in the Tribunal.

Mr Cooper has referred to Article 6 of the European Convention on Human Rights (ECHR), in order to fully understand the human rights compliance issues with this amendment. The right to fair trial is provided for in Article 6 of the ECHR. The reference in this right to an independent and impartial tribunal established by law has been interpreted to require that an independent and impartial tribunal is a competent one which necessitates that the tribunal is appropriately qualified. Mr Cooper states that a tribunal, for these purposes, need not necessarily be composed of professional judges, but the tribunal will need to have proven experience in the application of law.

²³ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.12

Mr Cooper's advice goes on to state:

It is acknowledged that there is an appeal from the Tribunal to the Jersey judicial system (on a point of law only), and, whilst this provides additional fair trial safeguards, it will not be enough, in my opinion, to cure any original structural defects in the first instance hearing. I am, therefore, of the view that this proposed amendment, without further safeguards being built in, could be challenged as violating both the right to a fair trial and the right to privacy, with its built in procedural safeguards, as guaranteed by the ECHR.

For this amendment to be compatible with the Human Rights (Jersey) Law, the authorities will have to be able to guarantee that the President is appropriately qualified and that the tribunal is competent to guarantee a fair hearing. There may be other provisions of Jersey law and practice that can be referred to that can ensure that the composition of the tribunal can guarantee the fairness of the hearing.

Mr Cooper concludes by recommending that before amendment two is put to the States, the removal of the professional requirement for the President of the Tribunal is reconsidered.

The Sub-Panel agrees with Mr Cooper that the removal of the professional requirement of seven years could have a significant effect regarding confidence levels in the Tribunal. It is interesting to note that the seven years is also requested under the UK Act which states that the person needs seven years' general qualification.

The Sub-Panel has taken into consideration the points Mr Cooper has raised, and believes that the Law should provide a degree of discretion, which would permit a candidate with at least three years experience to be considered if they were otherwise suitably qualified. The Sub-Panel also suggests that, whilst the person must be a locally qualified lawyer, the seven years' experience need not be as a locally qualified lawyer. The Sub-Panel considers it important to employ a President who is senior because effectively, he or she may need to overturn what the Commissioner has decided.

KEY FINDING

The Sub-Panel acknowledges that the UK Act applies the seven years required experience and accepts that by removing it from the Data Protection (Jersey) Law 2005, could affect confidence levels in the Tribunal.

RECOMMENDATION

The Sub-Panel recommends that the seven years required experience for the President of the Tribunal should remain however, a degree of discretion should be allowed. It also suggests that the Law should provide, in addition to discretion, that whilst the person must be a locally qualified lawyer, the seven years' experience need not be as a locally qualified lawyer.

8. AMENDMENT THREE

8.1 THE PROPOSAL

Amending the maximum penalty applicable to an offence under Article 55 of the Data Protection (Jersey) Law 2005; if this amendment was adopted, the maximum penalty would be increased to two years imprisonment and/or unlimited fine.

The Commissioner is requesting that a period of imprisonment and unlimited fine should be adopted under Article 55 of the Law:

“This is something that has been in the pipeline in the U.K. for some time and it is something that has been raised in meetings with the information commissioner and the other islands over the last couple of years. They have clearly been pushing for this amendment over there²⁴.”

It was also reasoned to be a deterrent factor:

“I will not use any names but, you know, ABC.com, if it is selling C.D’s or whatever and it has been offered £5,000 for 5,000 names to be sent to India, he is going to be sitting there, or she is, saying: “Well, is it worth my while if my company just gets fined or I might get the sack and I will go somewhere else”, but if he or she is going to be possibly hauled before a court and possibly imprisoned for a maximum of 2 years, there may well be a deterrent factor²⁵.”

The Sub-Panel accepts that amendment three of Article 55 may act as a deterrent, however, would like to note the uniqueness of a small jurisdiction such as Jersey. A balance needs to be struck as to how the legislation is used.

A letter received from the Minister for Home Affairs mentioned that he was advised that the draft Sex Offenders Law did not need to be re-drafted because the Data Protection Law would provide an appropriate remedy, provided that the penalties were increased:

“...I did indicate to the Assembly during the debate on the Sex Offenders (Jersey) Law 2010 that there were no specific criminal penalties for wrongful disclosure of information contained in that Law. It followed from this that we would be relying upon

²⁴ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.14

²⁵ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.14

the penalties created in the Data Protection Law. I then indicated that I was firmly of the view that these would need to be increased in order to include a power of imprisonment for up to a maximum of two years²⁶.”

In comparison, the Sub-Panel found it interesting that a maximum penalty for unlawful obtaining of data can also be seen in other legislation in Jersey. The *Banking Business (Depositors Compensation) (Jersey) Regulations 2010* were approved by the States on 3rd February 2010 and came into force on 10th February 2010:

14 Restricted information

(1) Except as provided by paragraphs (2) and (3), a person who receives information relating to the business or other affairs of a person –

(a) under or for the purposes of these Regulations; or

(b) directly or indirectly from a person who has received the information under or for the purposes of these Regulations,

is guilty of an offence and is liable to imprisonment for a term of 2 years and a fine if he or she discloses the information without the consent of the person to whom it relates and, if sub-paragraph (b) applies, the person from whom it was received²⁷.

If a maximum penalty of two years is found in other legislation in Jersey, the Sub-Panel are of the opinion that it would only be logical for legislation to complement one another.

DISCREPANCIES BETWEEN ARTICLES

Under Article 60 (false information) of the Law it states:

(2) Any person who knowingly or recklessly provides the Commissioner, or any other person entitled to information under this Law, with information that is false or misleading in a material particular shall be guilty of an offence if the information is provided in connection with an application under this Law.

(3) A person who is guilty of an offence against this Article shall be liable to a term of imprisonment of 5 years and to a fine.

²⁶ Letter from Minister for Home Affairs, 1st March 2010

²⁷ Draft Banking Business (Depositors Compensation) (Jersey) Regulations 200- p.16

The Sub-Panel wonders why the penalty for a person providing false or misleading information to the Commissioner is a penalty of five years and a fine, and the penalty, if amendment three was adopted, for unlawful obtaining of personal data under Article 55 is two years. As explained in Section 6, failure to comply with an information notice may be an offence under Article 55. However, Article 60 could potentially apply to failure to comply with information notices.

Under Article 47 of the Law it says that a person is guilty of an offence for failing to comply with an information notice. It also states that the person is guilty if a statement is made that the person knows to be false in a material respect:

47 Failure to comply with notice

- (1) A person who fails to comply with an enforcement notice, information notice or special information notice is guilty of an offence.*
- (2) A person is guilty of an offence if the person, in purported compliance with an information notice or special information notice –*
 - (a) makes a statement that the person knows to be false in a material respect; or*
 - (b) recklessly makes a statement that is false in a material respect.*
- (3) It is a defence for a person charged with an offence under paragraph (1) to prove that the person exercised all due diligence to comply with the notice in question.*

Both Article 60 and 47 refer to knowingly making false statements, and according to the Law it would seem that a person who knowingly makes a false statement to the Commissioner is liable for five years imprisonment, and a person who unlawfully obtains personal information is liable to two years imprisonment. The Sub-Panel questions this discrepancy between the Articles and strongly suggest that penalties for all breaches are clarified, before the amendment is lodged.

This discrepancy was also highlighted in Advocate Ruelle's report:

There appears, therefore, to be some inconsistency and uncertainty in the penalty that the Court may impose in relation to information notices, for example:

- *it is clear that failure to respond to an information notice at all is an offence for which the penalty is a fine;*
- *however, if an individual were to provide false information in response to an information notice, this appears to be an offence both under Article 47 and Article 60. It would appear to be the case that given the specific reference in Article 47 to offences in relation to providing false information in response to an information notice and that Article 60 is a more general offence, Article 47 would apply in these circumstances. If that is correct, then the penalty would be a fine alone. However, if a prosecution were instead to be brought under the provisions of Article 60, then the penalty would be up to 5 years imprisonment and/or an unlimited fine. It may, of course, be the case that offences in this regard would be committed under both Articles 47 and 60. This, however, leads to a situation where the penalties which may be imposed for essentially the same offence are dramatically different;*
- *a further difficulty arises in situations where an individual provides misleading information in response to an information notice. In this case, this would not constitute an offence under Article 47 (which only deals with the provision of false information) but it does appear to be caught by the offences set out in Article 60. In this circumstance, therefore, a person may be liable to a term of imprisonment of up to 5 years and an unlimited fine for providing misleading information when under Article 47 read in conjunction with Article 61, the penalty for providing false information, which would appear to be the more serious offence, is a fine alone.*

It is suggested that the issues relating to penalties for breach of Article 47 should be considered further if this amendment is to be adopted.

The Sub-Panel notes that a penalty of imprisonment refers to the maximum term which can be imposed for the offence, as set out in the “Interpretation (Jersey) Law 1954”.

KEY FINDING

The Sub-Panel is interested to note that there appears to be a discrepancy between Articles 60 and 55. A person may be liable to 2 years imprisonment under Article 55, but a person may also be liable to 5 years imprisonment under Article 60. Article 55 relates directly to an information notice whilst Article 60 may also potentially relate to an information notice.

RECOMMENDATION

The Sub-Panel recommend that penalties for all breaches are clarified before an amendment to increase the maximum penalty for offences under Article 55 is lodged.

8.2 DEPARTMENTAL EFFECTS

In his letter, the Minister for Home Affairs clarified that an increased penalty of two years imprisonment for unlawful obtaining would not have an impact on the States of Jersey Police or the HM Prison.

Statistics provided to the Sub-Panel from the States of Jersey Police indicate that since the introduction of the Law, there have been seven crimes recorded under Data Protection legislation in Jersey. Within the statistics it was also noted that an additional thirteen offences were recorded against the Computer Misuse (Jersey) Law 1995, where experience frequently revealed that such offences may originate from investigation of alleged breaches of the Law, according to the Acting Chief Officer.

When questioned about the effects amendment three would have on the business fraternity, the Minister for Economic Development was of the opinion that the current system of a fine was already 'appropriate':

"A law to be effective has to have again an appropriate sanction otherwise it is going to be open for abuse. I mean the level of financial penalty is probably more appropriate, I think. An imprisonment or potential imprisonment is quite a heavy sanction²⁸."

Further to the Public Hearing, the Minister for Economic Development provided a letter to the Sub-Panel (see appendix 7) which reiterated some of the concerns he expressed during the Hearing. Enclosed was also a letter from Jersey Finance, outlining its Members' concerns.

JERSEY FINANCE

Jersey Finance believes that a new amendment should be proposed, which would amend the obligation to make a notification. It believes that exemptions should be proposed to this clause in relation to where the personal data is kept:

²⁸ Transcript of Public Hearing Economic Development Department, 19th February p.6

1. in connection with the share and option plans for employee, directors and consultants of the company, any of its subsidiaries or any company in which the company is a shareholder (since participation in such plans is voluntary so any person will volunteer their personal data in order to participate); and
2. for any reason stipulated in a company's articles of association (Jersey listed PLC's often include provisions in their articles which seek to replicate provisions under English law which give rise to, for example, a shareholder to nominate a person to have "information rights" to receive notices of a meeting).

8.3 THE POSITION IN THE UK

In relation to Jersey's amendment three, sanctions currently available to the Information Commissioner in the UK under the UK Act are primarily concerned with bringing an organisation's future to comply with the UK Act. Mostly, they do not allow a penalty to be imposed for breaches that have already taken place. In some limited areas, the UK Act creates criminal offences, which may lead to prosecution. This is where the offence is sufficiently serious to warrant a criminal penalty. The principal offences are:

- Section 17 – processing without registration
- Section 55 – unlawful obtaining of personal data

These offences are currently punishable by a fine of up to £5000 in a Magistrates' court or an unlimited fine in the Crown Court. Similarly to Jersey, draft legislation to introduce the possibility of a custodial sentence for a section 55 offence is now before Parliament²⁹.

FREEDOM OF INFORMATION CAMPAIGN

As with amendment one, the Sub-Panel sought the views of Mr Maurice Frankel. Mr Frankel explained that a similar amendment to the UK Act has been enacted but not yet brought into force. According to Mr Frankel, the amendment in the UK has caused controversy because it is thought capable of affecting legitimate journalistic activity.

Mr Frankel goes on to say that the new and still dormant UK provision contains a safeguard for journalism not found in the current Jersey proposal. This takes the form of an improved public interest defence for a person who shows that he (a) acted for the 'special purposes'; (b) with a view to the publication of material for one of those purposes; and (c) in the *reasonable*

²⁹ Data Protection Powers and Penalties, The Case for Amending the Data Protection Act 1998, p.2

belief that in the particular circumstances the obtaining, disclosing or procuring [of the information] was justified as being in the public interest.

The Sub-Panel noted that this new defence is in addition to an existing public interest defence found in the UK Act and in Article 55(3)(d) of the Jersey Law. Both apply where disclosure can be shown to have been “justified as being in the public interest”. It is worth noting that the additional UK public interest defence goes beyond this, in that it introduces a “reasonable belief” element into the public interest test. Mr Frankel explains that this is intended, in part, to address concerns that legitimate journalistic activity might be otherwise inhibited by the existing public interest test.

Mr Frankel concludes by saying:

“The reasonable belief public interest test is still an objective test (i.e. the test is whether a reasonable person would have believed the disclosure to be in the public interest). If the current Jersey amendment is proceeded with there would be a strong argument for following the UK precedent and adding such “reasonable belief” public interest test to Article 55.”

The Sub-Panel noted that a public interest test is already found in Article 32(1)(b) of the Jersey Law, though it serves a different purpose there. It is interesting to note that the Commissioner commented on journalistic activity, when questioned about whether journalists are covered:

“Journalists are already covered. This would not add anything to journalists, no. Journalism is already covered³⁰.”

This issue was also highlighted by Advocate Ruelle:

Article 55 of the [Jersey] Law currently provides that a person will not commit an offence if the person can show that “in the circumstances of the case, the obtaining, disclosing or procuring was justified as being in the public interest.” There is no equivalent of the “reasonable belief” text.

³⁰ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.11

KEY FINDING

In comparison to the UK, the Sub-Panel has found that a “reasonable belief” Public interest test has not been added to the Data Protection (Jersey) Law 2005 under Article 55, to protection journalistic activity.

RECOMMENDATION

It is strongly recommended that Jersey should follow the UK precedent by adding a “reasonable belief” public interest test to Article 55 of the Law.

8.4 THE POSITION IN GUERNSEY

The Sub-Panel learned that Guernsey has already adopted an amendment that would add a prison sentence for a section 55 offence:

Assistant Commissioner, Guernsey:

“These amendments have been approved and are coming into force as from 01/03/10, i.e. within the next week. Then there will be prison sentences available for section 55 offences.

To date there has only been one prosecution under section 55 of our law. This concerned a policeman who disclosed the criminal record of his girlfriend to his live-in partner. He was found guilty of one count under section 55 and two counts under the Computer Misuse Law. He received a fine (about 2.5K) and was dismissed from the force.

I confirm that the penalties which Jersey is proposing for section 55 offences concur with the penalties to be available in Guernsey as from 01/03/10.”

8.5 HUMAN RIGHTS

Mr Cooper’s advice explains that presuming the sentencing powers are exercised proportionately; it is unlikely that any human rights concerns would arise under amendment three. He believes that this amendment would provide greater clarity and certainty.

KEY FINDING

Evidence suggests that increasing the penalty to two years imprisonment for unlawful obtaining would act as a deterrent. It was also noted that penalties of imprisonment are incorporated into other Jersey Legislation for Data Protection breaches.

RECOMMENDATION

The Sub-Panel recommend that there should be a public awareness campaign to address changes in the Data Protection Law. This could be beneficial because it could work in favour of the deterrence factor carried with some of the amendments.

9. AMENDMENT FOUR

9.1 THE PROPOSAL

Amending the power of seizure to include equipment found on premises; if this amendment was adopted, equipment as well as documents and “other material”, could be seized under a warrant.

This amendment was reasoned by the Commissioner as making the Law more “watertight”³¹.

“...if we are going in on a data protection issue and the only area where that data is present is on a computer, we want to take the computer, get the data, and return the equipment. The advice given to me is that it is probably okay to do that now but I do not want “probably”. I want “definitely”³².”

During the review the Sub-Panel found a potential loophole in relation to this amendment and Article 61, which concerns general provisions relating to offences. It states:

(3) *A court by or before which a person is convicted of –*

(a) *an offence under Article 21(1), 22(7), 55 or 56;*

(b) *an offence under Article 21(2) relating to processing that is assessable processing for the purposes of Article 22; or*

(c) *an offence under Article 47(1) relating to an enforcement notice,*

may order any document or other material used in connection with the processing of personal data and appearing to the court to be connected with the commission of the offence to be forfeited, destroyed or erased.

If the proposed amendment is clarifying the Law by adding equipment and separating it from other material, this could potentially cause problems in a Court of Law. Article 61 only refers to “*any document or other material*” which a Court may order relating to a case. The Sub-Panel question whether the person convicted could refuse to provide equipment on the basis of this loophole.

³¹ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.20

³² Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.19

The Sub-Panel are of the opinion that if equipment is included in Schedule 9, it should be included, where appropriate, in other provisions of the Law such as Article 61. Furthermore, it recommends that the Law should be revisited to ensure that there are no other incidences of potential loopholes.

Advocate Ruelle also mentions this loophole in her report:

On one reading of the Law, as drafted, there is some concern that given that equipment is mentioned only in the context of inspection, examination, operation and testing, the power to seize may not extend to equipment.

There is also, however, a suggestion that the power to seize "other materials" may extend to a power to seize equipment. However, there is a lack of certainty in this regard. The Sub-Panel heard evidence from the Commissioner that this lack of certainty is a concern especially given that much personal data is today stored and processed electronically.

It does, therefore, seem to be the case that this is a possible loophole which, for the sake of certainty and clarity, should be closed.

KEY FINDING

The Sub-Panel found a potential loophole regarding the amendment to include equipment found on premises rather than 'other material' and Article 61 of the Data Protection (Jersey) Law 2005, which refers to any documents and other material.

RECOMMENDATION

The Sub-Panel recommend that the word "equipment" is included in Article 61 to avoid any potential discrepancies in a Court of Law. Furthermore, it recommends that the Law should be revisited to ensure there are no other incidences of potential loopholes.

9.2 DEPARTMENTAL EFFECTS

The Sub-Panel sought the views of amendment four from the Minister for Home Affairs. In a letter provided to the Sub-Panel he asserted the proposed power would be used by the Commissioner:

"In relation to Amendment 4, the Police have already made the point that they have other more general powers of search under the PPCE [Police Procedures and Criminal Evidence] Law. The proposed powers would be used more so by the Data Protection

Registrar [Commissioner] if the Registrar were to develop an investigative role independent of that of the States of Jersey Police³³."

The Sub-Panel accepts the reasoning behind 'tightening up' the Law in Jersey however, it notes that the covering report states that there would be no financial or manpower implications for the States arising. The Sub-Panel is of the opinion that if an investigative role were adopted the Data Protection Office would require more resources. As per evidence obtained from the Public Hearing with the Commissioner would suggest that the office is already struggling (see section 6.3).

9.3 HUMAN RIGHTS

Mr Cooper believes that there are no particular human rights concerns with the fourth amendment, providing that it would be implemented proportionately with regard to privacy, property and fair trial rights.

³³ Letter from Minister for Home Affairs, 1st March 2010

10. AMENDMENT FIVE

10.1 THE PROPOSAL

Amending the maximum fee chargeable for subject access requests relating to health records; if this amendment was adopted, it would allow data controllers (who are required to respond to subject access requests relating to personal data defined as a health record) to charge a maximum of £50.

The year 2008 saw the end of the transitional period, in which the fee for subject access requests was brought down to £10.00. This followed the request from the Health and Social Services Department to the Commissioner for the fee to be raised back up to £50.00. The Commissioner had reasoned this amendment by stating that it was proposed because of a request from the Health and Social Services Department:

“So, the argument came to me, which I thought was very convincing, from Health that during the transition period of the law they had a maximum chargeable fee of £50 for their subject access requests.So I think they have a legitimate reason to ask for us to reconsider the £10³⁴.”

Even though the Commissioner believes that the Health and Social Services Department have a legitimate reason in requesting for the fee of £10 to be reconsidered, she also believes a fee of £10.00 is reasonable:

“£10 is very low but it is very low for a very good reason, that (a) to encourage organisations to have a good records management system so they can identify the data, but (b) it should not be a deterrent for people to exercise their own rights. So I think we have to find a balance...³⁵”

The Sub-Panel was concerned about specifically amending the fee for Health and Social Services records only. The Commissioner was asked whether there was a potential inequity between other people who also deal with complex data and health:

“Yes, to be brutally honest. There is and I think it is a question of looking at the arguments³⁶.”

³⁴ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.21

³⁵ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.22

³⁶ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.22

The Sub-Panel sought the opinion of the Deputy Commissioner in Ireland, as to what his views were on the Jersey amendments. In relation to amendment four he provided an email to the Sub-Panel which mentioned the EU Directive:

“The proposed amendments would seem to be very positive and should certainly be of assistance in enforcing data protection legislation. In this respect I know that Jersey has a finding of adequacy from the Commission under the EU Data Protection Directive. The only point I might make therefore would relate to the proposal to charge a fee of £50 for access to health related personal data. No doubt you have considered this in the context of Article 12...of that Directive which provides that personal data shall be supplied without excessive expense”.

The Sub-Panel noted that in Article 12 of the Data Protection Directive, it is the data subject’s rights of access to data. The Article states that Member States shall guarantee every data subject the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay or expense.

The Sub-Panel recognises that although the States of Jersey are in the process of looking at cost recovery, there is a need to emphasise Article 12 of the EU Directive. Costs should not prevent a subject from accessing their personal data.

10.2 DEPARTMENTAL EFFECTS

It was noted during the Public Hearing with the Minister for Health and Social Services, that there might be the possibility of a further request for the fee to be increased, as it does not cover the costs of the Department:

Expert Advisor:

“There seems to be not a lot of difference between £10 and £50...”

The Minister for Health and Social Services:

“... well, the law says £10 and to be up to £50, it is still not meeting the costs, especially of third party. The other 2 we can argue about but when you are looking at third party litigation, which Health just provides the information and that is it, £50 is not enough³⁷.”

³⁷ Transcript of Public Hearing Health and Social Services Department, 19th February p.10

The Minister for Health and Social Services provided the Sub-Panel with statistics as to the number of subject access requests that came into the Department in 2009:

Table 1: Approximate number of requests per year for records covered under Law

Type of Request	Amount of Requests in 2009
Third Party Litigation for example records of individuals involved in Road Traffic Accident and taking action against someone (non HSSD)	212
Individuals considering or taking legal action against Health and Social Services Department	65
Requests direct from patients themselves for copies of their records	122
Total	399

Table 2: Size of Request – Number of Pages

Size of Record Pages (between)	% of Requests
1 and 50	32.7%
50 and 100	18.3%
100 and 200	21.8%
200 and 300	11.9%
300 and 400	8.4%
400 and 500	3.0%
500 and 750	2.5%
930	0.5%
1280	0.5%
1626	0.5%

10.3 THE POSITION IN THE UK

The UK Act gives an individual the right to apply for a copy of personal information. A request would be made in writing, by letter or email, and sent it to the person or organisation that holds the information. Under the UK Act the organisation can ask for a fee of up to £10.00 for each request made.

In relation to health records, the UK Act gives an individual the right to see their health records. This would be in written format to the person or organisation concerned and would clearly describe the information sought. If the records are held on computer, an individual can be charged up to £10. If the records are manual or a mixture of manual and computer records, an individual can be charged up to £50. The individual would receive a reply to the request within 40 days.

10.4 THE POSITION IN IRELAND

Under Section 3 of the Data Protection Acts, an individual has the right to find out, free of charge, if a person (an individual or an organisation) holds information about them. An individual also has the right to be given a description of the information and to be told the purpose(s) for holding that information.

Under Section 4 of the Ireland Acts, an individual also has the right to get a copy of their personal information. This applies to all types of information for example, written details about an individual held electronically or on paper, photographs and CCTV images.

According to the Acts, an individual may have to pay a fee for some types of subject access request but this cannot exceed €6.35 (approximately £5.70).

In relation to health records, the Data Protection (Access Modification) (Health) Regulations, 1989 state that health data relating to an individual should not be made available to that individual, in response to an access request, if it was likely to cause serious harm to the physical or mental health of the data subject. It also states that a person who is not a health professional should not disclose health data to an individual without first consulting the individual's own doctor or some other suitably qualified health professional:

Explanatory Note

These regulations prohibit the supply of health data to a patient in response to a request for access if that would cause serious harm to his or her physical or mental

health. They provide also that such data is to be communicated only by, or after consultation with, an appropriate "health professional" — normally the patient's own doctor.

The Sub-Panel fully accepts the Irish Law in not charging a data subject for a request, however, believes that this would not be appropriate in Jersey. This point of view is supported by the evidence gathered during the Public Hearing with the Health and Social Services Department.

FREEDOM OF INFORMATION CAMPAIGN

Mr. Frankel considers amendment five questionable, on the grounds that even complex data may be reproduced on a CD (compact disc) lowering the cost considerably. Experience from the UK, he explains, often acts as a disproportionate barrier to people seeking their health records. The £50 charge has not been limited to complex forms of data, but has often been adopted as the standard charge, even for requests involving a few sheets of A4 paper. He provided an example of this:

"One NHS Trust in the UK has an online application form for patients seeking access to their health records. The first line of the form states: "Please Note: There is a charge for this service - £50 payable with requests, cheque payable to Stockport NHS Foundation Trust"

Mr. Frankel is also of the view that it would be unlikely that the Commissioner in Jersey would have any power to question even a clearly unreasonable £50 charge, for example, where the request was limited to a copy of a single letter from a hospital to the patient's GP.

He goes on to say that this amendment would also abolish the free access permitted to an individual's paper based health records, where these have been changed in the past 40 days³⁸. Such free access is permitted in the UK. The rationale is that the provision of information about their own health to patients currently undergoing treatment is good practice which should be encouraged, according to Mr. Frankel. The proposed change would make the Jersey provisions more restrictive in this respect than those in the UK.

[It was noted that Deputy M.R. Higgins dissented from recommendation 3.2.10 in relation to this amendment. He believes that the £10 fee should remain because he is opposed to

³⁸ Regulation 7(3) of the Data Protection (Subject Access Miscellaneous) (Jersey) Regulations 2005. The provision would be removed by the proposed amendment.

Health and Social Services charging higher for providing information to ordinary members of the public. He is also of the opinion that not all medical records would cost £50, as M.R.I (Magnetic Resonance Imaging) and C.T (Computerised Tomography) scans can be placed on DVD (Digital Versatile Disc). However, Deputy Higgins agreed to a £50 charge, in relation to third party requests for example law firms and insurance bodies.]

10.5 HUMAN RIGHTS

Mr Cooper recognises that the data protection directive requires that Member States guarantee every data subject the right to obtain from the controller data relating to him or her 'without excessive expense'. The issue relating to the £50 fee from a human rights perspective is the extent to which that fee will have an effect upon a data subject's right of access to data relating to them.

It is important to note that the data protection regime, even on an international level, envisages a fee, Mr Cooper believes that the issue is what the appropriate level ought to be. His view on this amendment is that it is not incompatible with Jersey's human rights obligations, however on a case-by-case basis he believes issues could arise. He then also said that Jersey authorities may wish to build in a degree of flexibility.

KEY FINDING

The Sub-Panel noted the inequity between Health and Social Services and other businesses for subject access requests. It was also noted that Jersey should follow the EU Data Protection Directive 95/46EC which states that data should be supplied without excessive expense. During the transitional period when the fee was a maximum of £50 the Health Department used their discretion, on what seemed to the Sub-Panel, a fair basis.

RECOMMENDATION

The Sub-Panel suggests that the maximum fee of £50 for subject access requests should be charged across the board. It further suggests that this should remain on a discretionary basis.

11. AMENDMENT SIX

11.1 THE PROPOSAL

Amending the provisions relating to subject access exemptions for trustees; if this amendment was adopted, it would allow restrictions on information provision relating to trustees (contained within the Foundation (Jersey) Law 2009) to be recognised within the Law.

This amendment would allow restrictions on information provision relating to trustees contained within the Foundation (Jersey) Law 2009 to be recognised within the Law. The Commissioner's reasoning for this amendment was that there are exemptions in the Foundations Law for the provision of information to individuals and there would be a risk of conflict if the two were not joined up.

"The Data Protection Law provides rights of access to information but if the trustees have been told not to provide that information to a beneficiary for certain reasons, by the settler or whatever, the Trust Law and the Foundations Law says that you are not obliged to disclose that. I think in the U.K. what had happened is some of the charities had sent round thousands of subject access requests to all trusts to see if they were going to benefit from any people's wills or trusts or whatever. So it would allow an exemption to the access request in relation to Foundations Law as it does now with Trust Law³⁹."

11.2 HUMAN RIGHTS

Initially, the Sub-Panel supported this amendment in respect of its purpose to 'tidy up' both Laws, and the reasoning behind it was therefore accepted. However, the legal opinion from Mr J. Cooper of Doughty Street Chambers suggests that this amendment may not comply with human rights.

Mr Cooper explains that amendment six cannot, without further explanation, be justified under human rights law. Article 7 of the Data Protection (Jersey) Law identifies that subject access is a fundamental right. Therefore, if Foundations are processing personal data, an individual who is affected by that processing of data must be able to make a subject access request.

³⁹ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.25

Even though there are exceptions to subject access provision, these are clearly defined. Mr Cooper goes on to explain that:

For this amendment to comply with Jersey's human rights obligations the Jersey authorities will need to give compelling reasons why the exemption is being proposed. A blanket exemption will almost certainly be found to be disproportionate. The Human Rights (Jersey) Law does anticipate the circumstances whereby the authorities may opt to introduce legislation in breach of the Convention, leaving the courts [European Court of Human Rights] with no alternative but to declare that legislation incompatible. However, this does not preclude a data subject from pursuing their claim before the Court. In the absence of compelling reasons for the exemption which are directly linked to those identified in the EU Data Protection Directive, the exemption will be found to violate Article 8 ECHR.

The Sub-Panel considered Article 8 of the European Convention on Human Rights to enhance its understanding of Mr Cooper's opinion on amendment six. Article 8 states:

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Sub-Panel accepts the opinion of Mr Cooper and acknowledge that he is relating the human rights issue to the Foundations (Jersey) Law 2009, as opposed to the Data Protection Law. Therefore, the Sub-Panel reiterate its original view that this amendment is not controversial. Advocate Ruelle also noted that Mr Cooper was referring to the Foundations Law:

*The Foundations (Jersey) Law 2009 (the "**Foundations Law**") provides that except as specifically required by or under the Foundations Law or by the charter or regulations of the foundation, a foundation is not required to provide any person (whether or not a beneficiary) with any information about the foundation. In particular, information about:-*

- (a) *the administration of the foundation;*
- (b) *the manner in which its assets are being administered;*
- (c) *its assets; and*
- (d) *the way in which it is carrying out its objects.*

That, of course, is without prejudice to any other obligation of a foundation to supply any information about the foundation imposed by an enactment or by an order of the court. An example of the latter may occur where a beneficiary has become entitled to a benefit in accordance with the charter or the regulations and the benefit is not provided.

The advice of Mr Cooper is noted in this regard. However, it would appear that to permit a data subject access request relating to personal data in respect of a foundation would be in direct conflict with the provisions of the Foundations Law. It should also be noted that a similar wholesale exemption is available in respect of trusts.

12. AMENDMENT SEVEN

12.1 THE PROPOSAL

Amending the provisions relating to subject access exemptions; if this amendment was adopted, it would add Article 41 of the Drug Trafficking Offences (Jersey) Law 1998 to the list of miscellaneous exemption contained within the Data Protection (Subject Access Exemptions) (Jersey) Regulations 2005.

The Sub-Panel noted that Article 41 of the Drug Trafficking Offences Law refers to ‘tipping off’.

Data Protection Commissioner:

“there are carve-outs for providing information under the Drug Trafficking Law which actually - and it is probably my fault, I shall probably have to take the blame for it - should have been put in the original law with Article 41 of the Drug Trafficking ... It is just to marry up the bits of legislation so that the Data Protection Law is not forcing someone to disclose information that another law is saying: “You must never disclose” so they sit comfortably⁴⁰.”

The Sub-Panel notes that this amendment is not contentious, and therefore accepts the reasoning behind it. This is also supported by Advocate Ruelle:

This amendment appears to be suggested because of an oversight in the original Law and is, in our view, uncontroversial. The amendment seeks to close a loophole whereby the Drug Trafficking Law prohibits certain disclosures but the Law would require that information to be disclosed as part of a data subject access request.

12.2 HUMAN RIGHTS

Amendment seven would be likely to fit within the general scheme of data protection, and will therefore be human rights compliant, according to Mr Cooper.

⁴⁰ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.24

13. AMENDMENT EIGHT

13.1 THE PROPOSAL

Amending the provisions relating to the notification fee from charities; if this amendment was adopted, it would allow data controllers whose sole processing activities relate to charity work to be exempt from the notification fee.

The Commissioner's reasoning for this amendment was that she did not feel right in taking money from charities:

"I am very conscious that I do not want to decrease the income, but my job is not just about getting money in, it is about doing morally what is right. And I think it feels better to me to say to places like Jersey Hospice that: "You have to notify with us. We have to know what you are doing because the nature of the data is so sensitive. Obviously the rules have to apply but we will not charge you." I would like that very much⁴¹."

13.2 DEPARTMENTAL EFFECTS

During the Hearing with the President of the Chamber of Commerce, the Sub-Panel learned that he had concerns about equality between charities being exempt and small businesses still having to pay:

"I know, for example, the chamber we do pay £50 a year, which I think we should be under the charities here but whether that will work I am not sure⁴²."

KEY FINDING

The Sub-Panel accepts that there may be an issue of inequality between charities being exempt from the notification fee, and small businesses.

RECOMMENDATION

The Sub-Panel considers charities being exempt from the notification fee as acceptable, however recommends that this is reviewed in the context of small businesses.

13.3 HUMAN RIGHTS

Mr Cooper states that no human rights concerns are engaged by the proposed eighth amendment.

⁴¹ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February p.25

⁴² Transcript of Public Hearing, Chamber of Commerce, 19th February p.2

14. PUBLIC AWARENESS

The Sub-Panel found during the review, that there may not be full awareness of data protection until it becomes apparent that it exists, such as publicised changes to the Law. This was highlighted in the Public Hearing with the Minister for Health and Social Services:

“It has been very interesting doing a bit of background research because data protection I think we just live with it and it just happens, so this has been quite a useful bit of research⁴³.”

Similarly to the Health and Social Services Department, the Sub-Panel learned during the Public Hearing with the President of the Chamber of Commerce, that people who own small businesses may not be aware of Data Protection:

“I do not think that a lot of our members, especially the smaller companies, are really very familiar at all with the Data Protection Law. It really does not come across their radar except if you are holding rather than account information, like in my day job, but depending on the size of your business as to whether or not you are registered with the Data Protection Authority and whether you pay the fees⁴⁴.”

The Commissioner mentioned that earlier on, her role was more proactive and she would educate people, particularly when the Law was adopted in 2005. However, evidence suggested that due to an increase in the complexity and number of complaints, the proactive aspect of the role had, because of prioritisation, taken second place to these complex issues:

“It has gone. Very rarely will you see us out talking to organisations now and if we do so we want a large audience so we can capture as many people as possible. In my first few years of being in the department I would go and talk to, you know, the church mouse if he asked me⁴⁵.”

The Sub-Panel hopes that there would be additional proactive work from the Commissioner and her Office. Educating the public and States of Jersey Departments would seem beneficial, taking into consideration the evidence heard in the Hearings.

⁴³ Transcript of Public Hearing, Health and Social Services Department, 19th February p. 2

⁴⁴ Transcript of Public Hearing Chamber of Commerce, 19th February, p. 2

⁴⁵ Transcript of Public Hearing, Treasury and Resources and Data Protection Commission, 19th February, p. 29

As previously mentioned, the Sub-Panel believe that there is an onus on the Data Protection Office to educate the public if any individual could be served with an information notice. However, if the Commission were to educate the public, this amendment would surely carry manpower implications on the Office:

“In terms of manpower implications no. I mean we do what we can do⁴⁶.”

KEY FINDING

Evidence from the Public Hearings suggested that there is a low level of awareness of Data Protection.

RECOMMENDATION

The Panel recommends that if the amendments were to be adopted, in particular amendment one, the general public and businesses need to be fully aware so that they can comply with the Law.

ECONOMIC DEVELOPMENT DEPARTMENT (“the Department”)

The Sub-Panel was somewhat disappointed to receive a letter from the Minister for Economic Development (see appendix 6) dated 23rd March 2010 which contradicted his opinion expressed in the earlier Public Hearing and in the letter which followed dated 3rd March 2010 (appendix 7).

The Sub-Panel noted that the Department took almost three weeks to provide it with the letter dated 23rd March 2010, even though there had been opportunities to provide the Sub-Panel with this information earlier. The Minister had the opportunity of expressing his opinion through a Public Hearing on the 19th February 2010, in which he disagreed with amendment one. The Sub-Panel wrote a letter to the Minister on the 23rd February 2010, to clarify what it had heard in the Public Hearing, and his response still stated the concerns he had raised during the Public Hearing.

The Minister has mentioned in his letter dated 23rd March, that he has since discussed amendment one with the Commissioner and “is persuaded⁴⁷” that the proposed extension is an appropriate means of dealing with the enforcement and compliance issues. The Sub-Panel found it interesting however, that in his previous letter, dated 3rd March, he states:

⁴⁶ Transcript of Public Hearing , Treasury and Resources and Data Protection Commission, 19th February, P.9

⁴⁷ Letter received from the Minister for Economic Development, 23rd March 2010 (appendix 6)

“Having looked into the matter further, I remain unconvinced of the need to extend the Commissioner’s power in relation to information notices so that such notices may be served on a person other than a data controller (or data processor)⁴⁸.”

The fact that the Minister has now had the opportunity to discuss the amendments with the Commissioner, and is now of a different opinion, highlights the Sub-Panel’s concern about awareness. It became apparent during the review that the Commissioner’s Office does not have the time or the resources to educate the public, however, the Sub-Panel feels that this is paramount. Not only does this relate to the public but also States of Jersey Departments, and they should be fully aware of data protection and the surrounding issues.

⁴⁸ Letter received from the Minister for Economic Development, 3rd March 2010 (appendix 7)

15. CONCLUSION

The Sub-Panel are in agreement with the majority of the amendments however, remain concerned with the wording of the draft legislation with amendment one. Noting that in other jurisdictions, privacy and electronic communications has come under the ambit of regulations due to the increasing world of technology. We would hope the Executive will consider the possibility of such regulations within Jersey.

The Sub-Panel have acknowledged the legal opinion expressed by Mr Cooper, that amendment one could enhance the data protection regime in Jersey, however, the Sub-Panel feel that the current format does not provide focus in the correct area. The ability to appeal against a notice is human rights compliant therefore awareness is paramount for the role of the Data Protection Tribunal and the confidence people have in it.

The Sub-Panel is in agreement with amendment three, due to its potential to act as a deterrent by increasing the maximum penalty to two years imprisonment however, further research found that the “reasonable belief” aspect for the public interest test was not within the realm of Article 55 of the Law.

There were potential discrepancies identified within both the accompanying report to the draft legislation and the draft legislation itself, which were highlighted after considering evidence from the Public Hearings and research into other jurisdictions.

The Sub-Panel’s advisor, Advocate Helen Ruelle shared some of the Sub-Panel’s concerns. She highlighted in her report that there appeared to be a lack of clarity in the Law relating to penalties for a breach of Article 47 and suggested that this is considered further if Article 43 is to be amended, as envisaged by amendment one. She also suggests that consideration is given to a requirement that the President of the Data Protection Tribunal is qualified as a lawyer for a specified period of time to try and meet the concerns expressed by Mr Cooper.

During the review the Sub-Panel recognised the impeccable work the Commission carries out and their ability to cope with such a large remit within a small team. The Sub-Panel would hope that the findings and recommendations produced from this report will go some way to assist the Data Protection Commissioner’s Office moving forward.

16. APPENDIX 1 – THE PROPOSED DATA PROTECTION AMENDMENTS



Proposed Amendments to the Data Protection (Jersey) Law 2005

REPORT

Current data protection legislation has been in force for over four years in Jersey.

In light of local regulatory experience and mindful of developments in other jurisdictions, the following proposed changes have been identified:

1. Amending the provisions in relation to information notices.

The draft Amendment Law would provide the Commissioner with the power to serve an information notice on a person other than a relevant data controller or data processor. This closely follows the position under section 12(1) of the Data Protection Acts 1988 and 2003 in Ireland and would not remove existing rights of appeal. Whilst it is recognised that the recent legislative changes in the United Kingdom (the Coroners and Justice Act 2009) do not reflect this, there are a number of policy reasons to support the proposed approach, including:

- The Commissioner has encountered difficulties in the course of investigation when applying existing legislation e.g. refusal by an individual to release relevant information results in an investigation being hampered;
- The UK Information Commissioner's Office has lobbied heavily for equivalent wording to that contained in the draft Amendment Law;
- The proposed amendment will lead to a more effective and proportionate regulatory environment (i.e. more limited recourse to "heavy duty" powers under the Data Protection (Jersey) Law 2005 e.g. involvement of police, obtaining of warrant etc).

2. Amending the professional requirements in relation to the President of the Data Protection Tribunal.

Removing the requirement for the President of the Data Protection Tribunal to be of seven years standing as an advocate or solicitor should provide greater latitude in the context of any future appointment process. It does not remove the requirement for a prospective appointee to be a local advocate or solicitor.

3. Amending the maximum penalty applicable to an offence under Article 55 of the Data Protection (Jersey) Law 2005.

The draft Amendment Law increases the maximum penalty to two years imprisonment and an unlimited fine. This is consistent with the position adopted in Guernsey in 2009. Similar measures are proposed in the United Kingdom. It recognises that the nature of the breaches in respect of data in this context are increasingly serious and the consequences severe. In addition, other legislation is increasingly looking to the Data Protection (Jersey) Law 2005 for remedy for serious data breaches.

4. Amending the power of seizure to include equipment found on premises.

The draft Amendment Law would ensure that equipment, as well as documents and "other material", is capable of being seized under a warrant. This is proposed as a result of increasing computerization of data and as such, the evidence which is required for an

investigation is rarely limited to documents. Again, existing safeguards have been retained.

5. Amending the maximum fee chargeable for subject access requests relating to Health Records.

The draft Amendment Law would allow data controllers who are required to respond to subject access requests relating to personal data defined as a health record to charge a maximum of £50. This recognises that health records are largely unique in their nature and supplying copies of the data contained therein requires significantly more resource than requests that relate to other data.

6. Amending the provisions relating to subject access exemptions for trustees

The draft Amendment Law would allow the restrictions on information provision relating to trustees contained within the Foundations (Jersey) Law 2009 to be recognised within the Data Protection (Jersey) Law 2005.

7. Amending the provisions relating to subject access exemptions

The draft Amendment Law would add Article 41 of the Drug Trafficking Offences (Jersey) Law 1998 to the list of miscellaneous exemptions contained within the Data Protection (Subject Access Exemptions)(Jersey) Regulations 2005.

8. Amending the provisions relating to the notification fee for charities

The draft Amendment Law would allow data controllers whose sole processing activities relate to charity work to be exempt from the notification fee.

Financial and manpower implications

There are no financial or manpower implications for the States arising.

European Convention on Human Rights

In the view of the Minister for Treasury and Resources, the provisions of the draft Data Protection (Amendment No.2)(Jersey) Law 201- are compatible with the Convention rights (as defined in Article 1 of the Human Rights (Jersey) Law 2000).



Jersey

DATA PROTECTION (AMENDMENT No. 2) (JERSEY) LAW 201-

Report

Explanatory Note

This draft Law amends the Data Protection (Jersey) Law 2005 (“principal Law”).

Article 1 is an interpretation provision.

Article 2 amends Article 43 of the principal Law by expanding the category of persons from whom the Data Protection Commissioner (“Commissioner”) can require information for an investigation whether data processing is being carried out in accordance with the data protection principles or otherwise in accordance with the principal Law. Currently Article 43 allows the Commissioner to serve notice requiring such information only on the “relevant data controller” (or data processor acting on behalf of the data controller). The amendment allows the Commissioner to serve notice on any person provided that the Commissioner regards the information sought as being relevant to the investigation and reasonably believes the recipient of the notice to have such information. The Commissioner is required to give reasons in the notice for thinking that the information sought is relevant.

Article 3 amends Article 55 of the principal Law by increasing the penalty for offences connected with unlawful disclosure of information. Under Article 61, the penalty for such offences is a fine. The amendment increases the penalty to a maximum of 2 years imprisonment and a fine.

Article 4 amends Schedule 5 of the principal Law in respect of the requirement that the President of the Data Protection Tribunal must be an advocate or solicitor of at least 7 years standing. Under the amendment no minimum length of time for qualification as an advocate or solicitor is required.

Article 5 amends Schedule 9 of the principal Law in 2 respects. First, the amendment makes it clear that the power to seize material from premises following the grant of a warrant extends to equipment found on the premises. Second, the Commissioner’s general powers in paragraph 14(1) of the Schedule relating to requiring information and documents in connection with the Commissioner’s investigation into an alleged offence are amended so as to remove an inconsistency relating to the inadvertent omission of a reference to information in sub-paragraph (1). (Both the heading and paragraph 14(3) currently refer to the power to require information.)

Article 6 cites the title of the draft Law and provides that it shall come into force 7 days after registration.



Jersey

DATA PROTECTION (AMENDMENT No. 2) (JERSEY) LAW 201-

Arrangement

Article

1	Interpretation	63
2	Article 43 amended	63
3	Article 55 amended	64
4	Schedule 5 amended	64
5	Schedule 9 amended	64
6	Citation and commencement	64



Jersey

DATA PROTECTION (AMENDMENT NO. 2) (JERSEY) LAW 201-

A LAW to amend the Data Protection (Jersey) Law 2005.

Adopted by the States [date to be inserted]

Sanctioned by Order of Her Majesty in Council [date to be inserted]

Registered by the Royal Court [date to be inserted]

THE STATES, subject to the sanction of Her Most Excellent Majesty in Council, have adopted the following Law –

1 Interpretation

In this Law “principal Law” means the Data Protection (Jersey) Law 2005.

2 Article 43 amended

In Article 43 of the principal Law –

(a) for paragraphs (1) and (2) there shall be substituted the following paragraphs –

“(1) If the Commissioner –

- (a) has received a request under Article 42 in respect of any processing of personal data; or
- (b) reasonably requires any information for the purpose of determining whether a data controller has complied, or is complying, with the data protection principles,

the Commissioner may serve notice on any person requiring that person to furnish to the Commissioner, in a specified form (if any) and within a specified period, specified information relating to the request or for the purpose described in sub-paragraph (b).

(2) An information notice shall contain –

(a) in the case referred to in paragraph (1)(a), a statement –

- (i) that the Commissioner has received a request under Article 42 in relation to the processing,
- (ii) that the Commissioner regards the specified information as relevant for the purpose of determining whether any processing (whether or not carried out by the person on whom the notice is served) has been or is being carried out in compliance with the provisions of the Law and the Commissioner’s reasons for regarding the specified information as being so relevant, and

- (iii) that the Commissioner reasonably believes the recipient of the notice to have the specified information; or
- (b) in the case referred to in paragraph (1)(b), a statement –
 - (i) that the Commissioner regards the specified information as relevant for the purpose of determining whether a data controller (whether or not the person on whom the notice is served) has complied or is complying with the data protection principles and the Commissioner’s reasons for regarding it as so relevant, and
 - (ii) that the Commissioner reasonably believes the recipient of the notice to have the specified information.”;

(b) for paragraph (11) there shall be substituted the following paragraph –

“(11) Nothing in paragraph (1) prevents the Commissioner from serving notices under that paragraph on more than one person, including on both a data controller and a data processor.”.

3 Article 55 amended

In Article 55 of the principal Law after paragraph (8) there shall be added the following paragraph –

“(9) A person guilty of an offence under this Article shall be liable to a term of imprisonment of 2 years and to a fine.”.

4 Schedule 5 amended

In paragraph 9(8) of Schedule 5 to the principal Law the words “of at least 7 years’ standing” shall be deleted.

5 Schedule 9 amended

In Schedule 9 of the principal Law –

(a) in paragraph 2(3) for the words “any documents” there shall be substituted the words “any documents, equipment”;

(b) for paragraph 14(1) there shall be substituted the following sub-paragraph –

“(1) The Commissioner may, for any purpose connected with the investigation of an offence under this Law or under Regulations made under this Law or with proceedings for such an offence, by notice in writing require any person to provide to the Commissioner, or any person appointed by the latter for that purpose, such information or documents, or both, as may be specified in the notice in such form (if any) and at such time and place specified in the notice.”.

6 Citation and commencement

This Law may be cited as the Data Protection (Amendment No. 2) (Jersey) Law 201- and shall come into force 7 days after it is registered.



Jersey

DATA PROTECTION (NOTIFICATION) (AMENDMENT) (JERSEY) REGULATIONS 201-

Report

Explanatory Note

These Regulations amend the Data Protection (Notification) (Jersey) Regulations 2005 in respect of the fees charged for a notification under Article 18 of the Data Protection (Jersey) Law 2005 by a data controller for inclusion in the register of data controllers. Under Article 18(5) of that Law a notification must be accompanied by any fee prescribed for that notification. (Such fee is currently £50).

Regulation 1 of the draft Regulations substitutes Regulation 6 of the Data Protection (Notification) Regulations 2005 so as to exempt, broadly speaking, charities from the requirement to pay a fee in respect of such a notification. More specifically, organizations, associations, trusts or non-profit organizations exempt from income tax under the provisions of the Income Tax (Jersey) Law 1961 relating to charities (such provisions being Article 115(a), (aa) and (ab) of that Law) are exempt from having to pay the fee except if the notification is given in the name of a school.

Regulation 2 of the draft Regulations sets out the title of the Regulations and says that they will come into force 7 days after they are made.



Jersey

DATA PROTECTION (NOTIFICATION) (AMENDMENT) (JERSEY) REGULATIONS 201-

Made

[date to be inserted]

Coming into force

[date to be inserted]

THE STATES, in pursuance of Articles 18 and 67 of the Data Protection (Jersey) Law 2005, have made the following Regulations –

1 Regulation 6 of the Data Protection (Notification) (Jersey) Regulations 2005 substituted

For Regulation 6 of the Data Protection (Notification) (Jersey) Regulations 2005 there shall be substituted the following Regulation –

“6 Fees to accompany notification under Article 18

- (1) Subject to paragraph (2), the prescribed fee to accompany any notification under Article 18 of the Law by a data controller (including a notification given in the name of a partnership in accordance with Regulation 4 or of a school in accordance with Regulation 5) is £50.
- (2) Paragraph (1) does not apply to a person who is a data controller for the purposes of any corporation, association, trust or non-profit organization exempt from income tax under Article 115(a), (aa) or (ab) of the Income Tax (Jersey) Law 1961 other than where notification is given in the name of a school in accordance with Regulation 5.
- (3) A fee that accompanies a notification shall be refunded if paid in mistake or (as the case requires) in the proportion in which it has been paid in mistake.”.

2 Citation and commencement

These Regulations may be cited as the Data Protection (Notification) (Amendment) (Jersey) Regulations 201- and shall come into force 7 days after they are made.



Jersey

**DATA PROTECTION (SUBJECT ACCESS
MISCELLANEOUS) (AMENDMENT) (JERSEY)
REGULATIONS 201-**

REPORT

Explanatory Note

These Regulations amend the Data Protection (Subject Access Miscellaneous) (Jersey) Regulations 2005 (“principal Regulations”) by prescribing £50 as the maximum fee that can be charged in respect of a subject access request that relates wholly or partly to personal data forming part of a health record. This provision replaces the transitional provision, now spent, in the principal Regulations relating to the prescribed fee for health records.



Jersey

DATA PROTECTION (SUBJECT ACCESS MISCELLANEOUS) (AMENDMENT) (JERSEY) REGULATIONS 201-

Made

[date to be inserted]

Coming into force

[date to be inserted]

THE STATES, in pursuance of Articles 7(4) and 67 of the Data Protection (Jersey) Law 2005, have made the following Regulations –

1 Data Protection (Subject Access Miscellaneous) (Jersey) Regulations 2005 amended

For Regulation 7 of the Data Protection (Subject Access Miscellaneous) (Jersey) Regulations 2005 there shall be substituted the following Regulation –

“7 Subject access requests in respect of health records

The prescribed maximum fee that a data controller may require in the case of a request made under Article 7(2)(a) of the Law, such request relating wholly or partly to personal data forming part of a health record, is £50.”

2 Citation and commencement

These Regulations may be cited as the Data Protection (Subject Access Miscellaneous) (Amendment) (Jersey) Regulations 201- and shall come into force 7 days after they are made.



Jersey

DATA PROTECTION (SUBJECT ACCESS EXEMPTIONS) (AMENDMENT) (JERSEY) REGULATIONS 201-

REPORT

Explanatory Note

Regulation 1 refers to the Data Protection (Subject Access Exemptions) (Jersey) Regulations 2005 as the “principal Regulations”.

Regulation 2 amends the principal Regulations so as to exempt from the subject access requirements of the Data Protection (Jersey) Law 2005 personal data in respect of a foundation.

Regulation 3 amends the principal Regulations so as to exempt from the subject access requirements of the Data Protection (Jersey) Law 2005 personal data the disclosure of which would be prohibited or restricted under Article 41 of the Drug Trafficking Offences (Jersey) Law 1988 (tipping off).

Regulation 4 sets out the title of these Regulations and provides that they shall come into force 7 days after they are made.



Jersey

DATA PROTECTION (SUBJECT ACCESS EXEMPTIONS) (AMENDMENT) (JERSEY) REGULATIONS 201-

Made

[date to be inserted]

Coming into force

[date to be inserted]

THE STATES, in pursuance of Articles 38 and 67 of the Data Protection (Jersey) Law 2005, have made the following Regulations –

1 Interpretation

In these Regulations “principal Regulations” mean the Data Protection (Subject Access Exemptions) (Jersey) Regulations 2005.

2 Regulation 1A inserted

After Regulation 1 of the principal Regulations there shall be inserted the following Regulation –

“1A Foundation exemption from Article 7

Personal data in respect of a foundation incorporated under the Foundations (Jersey) Law 2009 are exempt from Article 7 of the Data Protection (Jersey) Law 2005 to the extent that –

- (a) the personal data consist of information the withholding of which by the relevant data controller is authorized under Article 26 of the Foundations (Jersey) Law 2009; or
- (b) the personal data consist of information –
 - (i) the withholding of which by the relevant data controller is authorized by, or
 - (ii) the disclosure of which by the data controller would be contrary to a prohibition or restriction under,

any other enactment or rule of law (whether of Jersey or of another jurisdiction).”.

3 Regulation 2 amended

In Regulation 2(b) of the principal Regulations for the words “Article 44” there shall be substituted the words “Articles 41 and 44”.

4 Citation and commencement

These Regulations may be cited as the Data Protection (Subject Access Exemptions) (Amendment) (Jersey) Regulations 201- and shall come into force 7 days after they are made.

17. APPENDIX 2 – EVIDENCE CONSIDERED

The following documents are available to read on the Scrutiny website (www.scrutiny.gov.je) unless received under a confidential agreement.

Documents

1. The Data Protection (Jersey) Law 2005 (as amended)
2. The Guide to Data Protection (2009) Information Commissioner's Office
3. Information Commissioner's Office Annual Report 2008/09
4. Data Protection Powers and Penalties, The Case for Amending the Data Protection Act 1998, Information Commissioner's Office
5. Data Protection in the European Union, European Commission Office UK
6. The Office of the Data Protection Commissioner, Annual Report 2008
7. Draft Banking Business (Depositors Compensation) (Jersey) Regulations 200-
8. The Campaign for Freedom of Information submission
9. Ministry of Justice, Impact Assessment on Enhancing the Commissioner's Inspection Powers with the Data Protection Act 1998
10. Draft Banking Business - Depositor Compensation Jersey Regulations
11. European Parliament Report to the Implementation of the Data Protection Directive 9546EC

Public Hearings

19th February 2010

1. Deputy A.E. Pryke, Minister for Health and Social Services
Ms M. Cabot, Information Governance Manager
2. Mr R. Shead, President, Chamber of Commerce
3. Senator A.J.H Maclean, Minister for Economic Development
Mr J. Mews, Director, Finance Industry Development
4. Deputy E. J. Noel, Assistant Minister for Treasury and Resources
Mrs E. Martins, Data Protection Commissioner

A verbatim transcript of the Public Hearings is available on the Scrutiny website (www.scrutiny.gov.je).

18. APPENDIX 3 – GLOSSARY OF TERMS

Data Controller: 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 who processes the data on behalf of a data controller, but does not include an employee of the data controller;

Data subject: the living individual who is the subject of the personal information (data).

Information notice: is a written notice from the Commissioner to a data controller or a public authority seeking information that the Commissioner needs to carry out her functions. Failure to comply with an information notice is an offence.

Notification: is the process by which a data controller's processing details are added to a register. Under the Data Protection (Jersey) Law 2005 every data controller who is processing personal information needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a data controller is exempt from notification, they must still comply with the data protection principles.

Personal data: is information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession

Processing: is obtaining, recording or holding the data or carrying out any operation or set of operations on data.

European Convention on Human Rights: an official agreement signed by the UK and most other European countries, in which they promise to allow every citizen their human rights, such as the right to be free, to express their political opinions, and to be treated fairly.

19. APPENDIX 4 – Jonathan Cooper’s Human Rights Legal Opinion

Re: The Data Protection Sub-Panel of the States of Jersey

Proposed Amendments to the Data Protection (Jersey) Law 2005

Opinion

1. I have been asked to advise the Data Protection Sub-Panel of the Corporate Services Panel of the States of Jersey on the human rights compatibility of proposed amendments to the Data Protection (Jersey) Law 2005.
2. Human rights compliance, for these purposes, will be premised upon the Human Rights (Jersey) Law 2000. Eight amendments are being proposed. These have been set out in a Report produced under the auspices of Jersey’s Data Protection Commissioner. I have also been sent the draft legislation relating to the proposed amendments.
3. The first amendment relates to whom information notices can be served. The second concerns the professional requirements for the President of the Data Protection Tribunal. The third amendment seeks to codify the maximum criminal penalties available for offences committed under the Law. The fourth extends the seizure powers under the Law. The fifth amendments relates to increasing the fee chargeable to subject access requests relating to health records. The sixth would exempt, to all intents and purposes, foundations under the Foundations (Jersey) Law 2009 from the scope of the Data Protection (Jersey) Law 2005. The seventh amendment would add Article 41 of the Drug Trafficking Offences (Jersey) Law 1988 to the list of miscellaneous exemptions contained within the Data Protection (Subject Access Exemptions)(Jersey) Regulations 2005. Finally, the eighth amendment waives the notification fee under the Law for charities.
4. The effect of Article 16 of the Human Rights (Jersey) Law 2000, which obliges a Committee which is lodging *au Greffe a projet de loi* to make a statement of compatibility before the second reading of the *projet*,⁴⁹ is that the Jersey legislature should be confident that the draft legislation that they are passing into law is human rights compliant, thus preventing (as best the States of Jersey can) human rights violations occurring in the first place. This advice should assist the States of Jersey examine the human rights compliance of the proposed amendments.

Summary of the advice

5. The majority of the amendments raise nominal or no serious human rights concerns; however, in relation to two of the amendments it is advised that a more detailed human rights assessment of the proposed measures is prepared by the Jersey authorities. These amendments, on their face, are not compatible with Jersey’s human rights obligations and the appropriate authorities need, therefore, to provide clearer justifications for the measures proposed and to explain in detail why they

⁴⁹ A statement under Article 16(1)(a) or Article 16(1)(b) can be made

consider them to be human rights compliant. Once that exercise is carried out, an Article 16 statement of compatibility, either under Article 16 (1)(a) or (b) can be made.

6. The amendments of particular concern in the above list relate to the professional requirements of the Tribunal President and the effective exemption of Foundations from the scope of the Data Protection (Jersey) Law. Both of these potentially raise serious human rights concerns, whereby the amendment itself (if passed into law) could be found in breach of the Human Rights (Jersey) Law 2000. Consequently, there are doubts that these amendments, as currently formulated, could be given a statement of compatibility under Article 16 of that Law.
7. In relation to the other amendments that raise aspects of human rights protection, any concerns about the amendments themselves will not be substantive. Issues about how the particular Article or provision will be implemented may require scrutiny. As public authorities in Jersey are required to act in a way that is compatible with the Human Rights (Jersey) Law 2000, including the Data Protection Commissioner, it can be assumed with confidence that those amendments will be implemented in a way that protects the human rights of all concerned.
8. There could be human rights issues raised by the extension of those to whom information notices can be served, as well as the fees chargeable for access to health records, but it is expected that these would be addressed by the way in which those provisions will be implemented. Exempting the tipping off provision contained in Article 41 of the Drug Trafficking Offences (Jersey) Law 1988 from the Data Protection regime would be likely to fit within the general scheme of data protection and will, therefore, be human rights compliant. If this exemption touches on the fairness of a trial, it can be assumed, again with confidence, that the Jersey authorities will ensure the fairness of any trial.
9. As it would be expected that the sentencing powers provided for by the third amendment would be exercised proportionately, it is unlikely that any human rights concerns would arise under this amendment and the amendment itself provides for greater clarity and certainty. Similarly, assuming that the fourth amendment would be implemented proportionately with due regard to privacy, property and fair trial rights, no particular human rights concerns arise. No human rights concerns are engaged by the proposed eighth amendment.

Human Rights Standards Applicable to Data Protection

10. The key human rights standards contained in the Human Rights (Jersey) Law 2000, which are relevant to the proposed amendments to the Data Protection (Jersey) Law 2005 are: the right to respect for private life, as provided for by Article 8 of the European Convention on Human Rights (ECHR); the right to a fair trial contained in Article 6 ECHR; the right to freedom of expression guaranteed by Article 10 ECHR; and the prohibition on discrimination provided for by Article 14 ECHR. The right to property provided for by Article 1 of the First Protocol of the ECHR will also be relevant. There is a secondary issue in relation to property rights which is the extent to which information itself is property. This will not be considered in this advice.

11. The Data Protection (Jersey) Law 2005 is designed, in principle at least, to give effect to key aspects of privacy protection as guaranteed by Article 8 ECHR. Article 8 states:
 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
 2. There shall be no interference by a public authority with the exercise of this right, except such as is in accordance with the law and is necessary in a democratic society, in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
12. The proposed amendments to be human rights compliant must, therefore, be in keeping with both the letter and the spirit of Article 8. It is worth emphasising that protecting privacy in the information age is recognised as being a key aspect of human rights protection in the 21st century. The primary purpose of the Data Protection (Jersey) Law is recognition of this fact; although it is also accepted that there is a secondary function to the law that enables a consistent approach to data protection to be carried out across the European region. There is, therefore, a commercial, or corporate, imperative for coherent and consistent data protection provisions.
13. Whilst the foundation of data protection from a European human rights perspective is Article 8 ECHR,⁵⁰ its construction lies in the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data 1981. In turn, the human rights provisions of that Convention were enhanced and improved upon at the EU level by the Data Protection Directive, which was adopted on 24 October 1995.⁵¹ This Directive was, in turn, given UK domestic effect by the Data Protection Act 1998 (DPA), which repealed and replaced its 1984 predecessor. The Data Protection (Jersey) Law is closely modelled on the DPA 1998. Its origins, which it acknowledges, lie therefore in the Directive and the Council of Europe Convention before that.
14. When assessing any data protection matter for compliance with human rights standards, the starting point must be Article 8 ECHR, but that enquiry will be insufficient if it does not include an examination of both the Council of Europe Convention as well as the Directive. This, in turn, means that not only must the ECHR be followed as a matter of Jersey law, but so too the EU Charter of Fundamental Rights and Freedoms must be taken into account.⁵² The Directive, as EU law, will be interpreted in the light of the Charter. Article 8 ECHR will be similarly interpreted in light of the Charter's provisions.
15. The EU Charter provides numerous safeguards in relation to data protection. Not only is there a comparable provision to Article 8 ECHR (Article 7 of the EU Charter) guaranteeing respect for private life, the Charter in its Article 8 provides express protection for personal data. That Article 8 is as follows:

⁵⁰ Comparable privacy protection exists at the UN level. See Article 17 ICCPR.

⁵¹ Directive 95/46/EC, OJ 1995 L 281/31.

⁵² The EU Charter became a binding part of EU law through the Lisbon Treaty which entered into force on 1 December 2009.

1. Everyone has the right to the protection of personal data concerning him or her.
 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified.
 3. Compliance with these rules shall be subject to the control of an independent authority.
16. This provision in Article 8 of the EU Charter both mirrors and must be read into the case law under Article 8 ECHR.⁵³ Article 8 of the EU Charter is, therefore, confirming, as well as clarifying, the scope of Article 8 ECHR as it relates to data protection.
17. Other articles in the EU Charter relevant to data protection are a more comprehensive right to a fair trial in Article 47 of the Charter than that which is provided for by Article 6 ECHR. There are wide-ranging equality and non-discrimination provisions in the Charter, and importantly there is a right to good administration (Article 41). Article 42 also provides a right of access to documents held by EU agencies.
18. In making these references to the EU Charter it must be stressed that the Charter (for these purposes) only applies to the implementation of EU law.⁵⁴ It is also acknowledged that Jersey is not a Member State of the European Union, although it has its own particular relationship with the EU. However, should there be challenges to the proposed amendments if they are passed into law, any legal challenge will inevitably rely upon the EU Charter as a source of law. If nothing else it will be considered to be highly persuasive in understanding how the law of data protection is to develop and be interpreted.
19. Freedom of expression will also be relevant in the context of data protection, but freedom of expression, in and of itself, cannot justify a violation of data protection principles.⁵⁵ Further sources of human rights law relating to data protection come also from the UN as well as the OECD. These sources of law will not be relied upon for this advice.
20. Data protection laws, whilst forming a crucial aspect of the right to privacy, are not substantive privacy laws as such. Data protection provides procedural safeguards in relation to the extent to which personal information is disseminated to other people. Consequently, procedural fairness, hence principles linked to the right to a fair trial (and the right to good administration), is a central component of data protection as a human rights issue.
21. Whilst it is beyond the scope of this advice, for data protection to be fully effective as a human rights issue, it should be coupled with a right to freedom of information. The imbalance in Jersey law as it currently stands, where there are no express provision

⁵³ See the Explanations to the EU Charter. ECHR case law cited in this advice can be found at the HUDOCS website of the European Court of Human Rights: <http://cmiskp.echr.coe.int/tkp197/search.asp>. This website is very easy to navigate and it is self explanatory.

⁵⁴ Article 51 (1) of the EU Charter. The UK has also negotiated a Protocol in relation to the interpretation of the EU Charter; however, this Protocol is not an opt-out from the Charter and the Charter still applies within the UK.

⁵⁵ *Campbell v. MGN Mirror Group Newspapers Ltd.* [2004] UKHL 22

guaranteeing freedom of information, means that this aspect of human rights protection within Jersey is incomplete. Even though the ECHR does not provide for an express right of freedom of information, recent case law before the European Court of Human Rights (the Court) has suggested that such a right can be read into Article 10 ECHR (freedom of expression), and the Jersey authorities should be aware that these developments might force a freedom of information law upon them.⁵⁶

A Human Rights Audit of the Proposed Amendments

22. Inevitably, there will be competing policy considerations in relation to the proposed amendments. This advice will not touch upon these or speculate on the merits or otherwise of the amendments. Its aim is only to identify and clarify any human rights issues which may arise.
23. As already mentioned above, some of the amendments could raise human rights concerns if they are implemented in a manner which violates the Human Rights (Jersey) Law. Article 7(1) of that Law, however, requires that all public authorities act in a way which is compatible with the rights contained within the Law; therefore, it can be asserted with confidence that any public authority implementing the data protection regime in Jersey will do so in a human rights compliant way. Ultimately, the courts will provide guidance and, if necessary, impose coercive measures to ensure this obligation is carried out. The only exception to this obligation to act in a way that is compatible with the human rights standards contained in the Law is where a Law is clear on its face and requires a public authority to act in a manner which is inconsistent with human rights protection (Article 4). Under these circumstances the appropriate court is entitled to declare that legislation incompatible with the rights contained in the Law (Article 5).
24. In auditing the proposed amendments for human rights compliance, this advice will follow the same structure that the Data Protection Commissioner has used in her Report on those amendments in terms of the ordering and numbering of them.

Amendment 1: Amending the provisions in relation to information notices

25. Human rights law is not prescriptive about how data protection regimes are implemented within national jurisdictions. Human rights law is only concerned that those regimes are effective in controlling the extent to which personal information is disseminated to other people. Data protection seeks to give an individual a greater measure of control over personal information and to place controls over the dissemination of this information. Human rights law oversees this process.
26. Human rights law sets down a basic minimum standard that must be met. For example, both the Council of Europe Data Protection Convention and the EU Directive provide for a broader range of protection than was subsequently incorporated into the UK's DPA 1998. This does not mean that the UK's DPA is necessarily in violation of the UK's human rights obligations. It does, however,

⁵⁶ *Sdruženi Jihočeské Matky v Czech Republic; Kenedi v Hungary; HCLU v Hungary*

indicate that the UK does not safeguard data protection as comprehensively as other jurisdictions.

27. The proposed amendment, which gives the Commissioner the power to serve an information notice on those who may be processing data unlawfully other than the data controller and the data processor, goes beyond the provisions of the UK's DPA. The latter is limited to serving information notices only on data controllers and data processors. There is, however, nothing to prevent the Jersey authorities from providing greater human rights protection (even though this may raise consistency issues between the UK and Jersey). In my view the proposed amendment to Article 43 is consistent with Article 8 ECHR, which will be interpreted in the light of Article 8 of the EU Charter. As the Commissioner points out, it will give her more effective tools to regulate data protection more effectively.
28. Clearly, when the Commissioner is implementing powers under amended Article 43, assuming it enters into law, the Commissioner will act in a way that is compatible with all human rights for all who are affected by her decision. Most notably, if the information notice is to be served on a media organisation, she will ensure that her actions comply with her responsibilities under Article 10 ECHR, as well as Article 12 of the Human Rights (Jersey) Law.
29. It is my view, therefore, that Article 43 as amended, and coupled with existing safeguards built into the Law, which guarantee a right to appeal,⁵⁷ and the suspension of the process whilst the appeal is pending,⁵⁸ as well as the duty to make a statement explaining why the information notice is being served,⁵⁹ will enhance the data protection regime in Jersey. It is, therefore, adding to human rights protection, which is welcomed, not limiting it.

Amendment 2: Amending the professional requirements in relation to the President of the Data Protection Tribunal

30. This amendment proposes to remove the requirement for the President of the Data Protection Tribunal to be of seven years standing as an advocate or solicitor.
31. As is evidenced by Article 8(3) of the EU Charter, the success of any data protection regime is predicated on the fact that this regime is subject to the control of an independent authority. For both Jersey and the UK, this protection does not just include the creation of the Commissioner; it also ultimately rests upon the tribunal which is an integral part of both legislative schemes. For that independent authority to be effective it must be competent. This includes not just the Commissioner, but also the tribunal. Competence requires that the authority is appropriately qualified.
32. The creation of the independent tribunal provided for by Article 6 of the Data Protection (Jersey) Law (the appointment to which is governed by paragraph 9 of Schedule 5), reflects the earliest cases before the Court concerning matters relating to personal information and data protection. In *Gaskin v. UK* the Court affirmed that the role of the independent authority in determining matters relating to data protection was as, if not more, important than the data protection provisions in and of

⁵⁷ Article 48, Data Protection (Jersey) Law 2005

⁵⁸ Article 43(4), *ibid.* See also Articles 43(5) & (6)

⁵⁹ Proposed amendment to Article 43(2) see Article 2, Data Protection (Amendment No. 2)(Jersey) Law 201-

themselves. The independence of that authority is guaranteed by having an appeal from it to an independent tribunal.

33. The Data Protection Tribunal will, by definition, be dealing with matters of law and fact of significant complexity. If the proposed amendment to Article 43 is accepted, that complexity will be increased. Therefore, the President of the Tribunal has to have sufficient standing, as well as its appearance, to be able to manage these issues and inspire confidence in all concerned. Removing the professional requirement qualification of seven years' standing could undermine confidence in the Tribunal.
34. To understand fully the human rights compliance issues in relation to this amendment, reference should be had to Article 6 ECHR and the right to a fair trial. The reference in this right to an independent and impartial tribunal established by law has been interpreted to require that an independent and impartial tribunal is a competent one which necessitates that the tribunal is appropriately qualified.⁶⁰ A tribunal, for these purposes, need not necessarily be composed of professional judges, but the tribunal will need to have proven experience in the application of law. It is acknowledged that there is an appeal from the Tribunal to the Jersey judicial system (on a point of law only), and, whilst this provides additional fair trial safeguards, it will not be enough, in my opinion, to cure any original structural defects in the first instance hearing. I am, therefore, of the view that this proposed amendment, without further safeguards being built in, could be challenged as violating both the right to a fair trial and the right to privacy, with its built in procedural safeguards, as guaranteed by the ECHR.
35. For this amendment to be compatible with the Human Rights (Jersey) Law, the authorities will have to be able to guarantee that the President is appropriately qualified and that the tribunal is competent to guarantee a fair hearing. There may be other provisions of Jersey law and practice that can be referred to that can ensure that the composition of the tribunal can guarantee the fairness of the hearing.

Amendment 3: Amending the maximum penalty applicable to an offence under Article 55 of the Data Protection (Jersey) Law 2005

36. Sentencing provisions of this nature add certainty and clarity to the creation of criminal offences. It is, therefore, to be welcomed. From a human rights perspective, the prospect of a two-year custodial sentence for the most serious breaches of data protection, with their self-evident human cost, would not appear to be too extreme to amount to a disproportionate penalty. Once again, the EU Charter will be of assistance in interpreting this provision. Article 49(3) of that Charter states that the severity of penalties must not be disproportionate to the criminal offence. For further clarity, it may be appropriate to identify that the fine envisaged under amended Article 55 could be unlimited. The size of the fine will, of course, be dependent upon the seriousness of the facts, the extent of the data protection violation and its consequences.

⁶⁰ UN Basic Principles on the Independence of the Judiciary, Article 10. See also Opinion no 1 (2001) of the Council of Europe's Consultative Council of European Judges (CCJE), on Standards Concerning the Independence of the Judiciary and the Irremovability of judges Recommendation no. r (94) 12.

37. I am confident that the Jersey courts would apply their sentencing powers proportionately, taking into account the scope of human rights protection contained in the Human Rights (Jersey) Law, and that sentencing under amended Article 55 would be proportionate. Therefore, the application of Article 55 in practice is unlikely to raise any significant human rights concerns.

Amendment 4: Amending the power of seizure to include equipment found on premises

38. The draft Amendment Law would ensure that equipment, as well as documents, is capable of being seized under a warrant. This amendment is improving the ability of the Commissioner to carry out her functions. Safeguards are in place and there is express provision relating to the protection of privacy rights. In my opinion, this amendment seeks to implement more effectively Article 8 of the EU Charter.

39. There are risks attached to the seizure of equipment as envisaged by this amendment, most notably in respect of the protection of privacy rights of third parties; however, it can be expected that the Commissioner will be fully cognisant of these issues and will have mechanisms in place to protect the privacy rights of third parties in relation to seized equipment and other material.⁶¹

40. The seizure of this equipment will raise issues of property rights, both in the context of the equipment itself and the extent to which information can be categorised as property. Seizure of property under these circumstances may or may not amount to a deprivation of property or it may amount to a regulation of property. Article 1 of the First Protocol ECHR does permit both the deprivation and regulation of property. As a general principle of human rights law property may be confiscated and/or regulated by law where this is necessary for the public interest. The lawful application of these provisions will, therefore, not violate the ECHR.

Amendment 5: Amending the maximum fee chargeable for subject access requests relating to health records

41. The draft Amendment Law would allow data controllers who are required to respond to subject access requests relating to personal data defined as a health record to charge a maximum of £50.

42. The Data Protection Directive requires that Member States guarantee every data subject the right to obtain from the controller data relating to him (or her) 'without excessive expense'. This principle is recognised in Article 7(4)(b) of the Data Protection (Jersey) Law. The issue relating to the £50 fee from a human rights perspective is the extent to which that fee will have a chilling effect upon a data subject's rights of access to data relating to them.

43. The regime, even at an international level, clearly envisages a fee; the issue is what the appropriate level ought to be. It should be born in mind that those with disabilities who may wish access to their health records, which is likely to be sensitive personal information, will be more likely to be living on lower incomes. A question, therefore, will arise whether a fee of £50 will become an impediment to access. The role of the Jersey authorities should be to facilitate access to data protection in order to meet its obligations fully under Article 8 ECHR as interpreted by Article 8 of the EU Charter.

⁶¹ See, for example, *Niemitz v. Germany*.

44. One option may be to provide for a waiver of the fee in certain circumstances; another could be to adhere to a clearly graduated fee structure. The risk will be that all data subject requests for medical records will be charged at £50.00.
45. On its face this amendment is not incompatible with Jersey's human rights obligations; however, on a case-by-case basis issues may arise, and the Jersey authorities may wish to build in a degree of flexibility in relation to the fees charged.

Amendment 6: Amending the provisions relating to subject access exemptions for trustees under the Foundations (Jersey) Law 2009

46. The draft Amendment Law would allow the restrictions on information provision relating to trustees contained within the Foundations (Jersey) Law 2009 to be recognised within the Data Protection (Jersey) Law 2005.
47. This exemption or exception to subject access provisions in relation to Foundations as governed by the Foundations (Jersey) Law 2009 cannot on its face, without further explanation, be justified under human rights law. In my opinion, if the Jersey authorities wish to pursue this matter and make this provision law, a statement of compatibility under Article 16(1)(b) of the Human Rights (Jersey) Law 2000 will have to be made.
48. As Article 7 of the Data Protection (Jersey) Law identifies, subject access is a fundamental right. Therefore, if Foundations are processing personal data, an individual who is affected by that processing of data must be able to make a subject access request. It is worth recalling the pre-eminence that the Court gives to data protection. In *S & Marper v. UK* it was stated that 'the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention'.⁶²
49. Whilst the data protection regime does accept that there can be exceptions to subject access provisions, these are clearly defined and, even then, they are subject to the tests of necessity and proportionality.⁶³ The Data Protection Directive allows Member States to provide exemptions from subject access when this constitutes a necessary measure to safeguard one or more of seven grounds. These include national security, public security, prevention, investigation, detection and prosecution of criminal offences, an important economic or financial interest and/or the protection of the data subject or the rights and freedoms of others.⁶⁴
50. For this amendment to comply with Jersey's human rights obligations the Jersey authorities will need to give compelling reasons why the exemption is being proposed. A blanket exemption will almost certainly be found to be disproportionate. The Human Rights (Jersey) Law does anticipate the circumstances whereby the authorities may opt to introduce legislation in breach of the Convention, leaving the courts with no alternative but to declare that legislation incompatible. However, this does not preclude a data subject from pursuing their claim before the Court. In the absence of compelling reasons for the exemption which are directly linked to those

⁶² Para. 103.

⁶³ *Baker v. Secretary of State for the Home Department* [2001] UKHRR 1275. That case held that even under national security, cases must be considered on a case by case basis.

⁶⁴ Directive 95/46/EC, Article 13(1).

identified in the EU Data Protection Directive, the exemption will be found to violate Article 8 ECHR.

51. A further concern that the Jersey authorities may wish to consider is the discrimination arguments that may also be raised under Article 14 ECHR as read with Article 8. The authorities would, therefore, have to justify any difference of treatment in relation to data subject access rights to non-Foundations as opposed to Foundations.

Amendment 7: Amending the provisions relating to subject access exemptions in relation to drug trafficking offences

52. The draft Amendment Law would add Article 41 of the Drug Trafficking Offences (Jersey) Law 1988 to the list of miscellaneous exemptions contained within the Data Protection (Subject Access Exemptions)(Jersey) Regulations 2005.

53. As has already been identified in relation to amendment 6, it is possible to exempt subject access in relation to prevention, investigation, detection and prosecution of criminal offences. The mischief which Article 41 of the Drug Trafficking Offences (Jersey) Law addresses (tipping off) is a necessary part of the framework to control drug trafficking. Under the circumstances, therefore, the inclusion of Article 41 within the Data Protection (Subject Access Exemptions) (Jersey) Regulations would be likely to be compliant with international human rights standards.

54. One possibility is that a defendant who is being prosecuted under Article 41 of the Drug Trafficking Offences (Jersey) Law might seek to argue that the exemption undermines his or her right to a fair trial. In my opinion such an argument would be a red herring and could be easily dismissed. However, for completeness, I will address the issue here.

55. The right to a fair trial, with its built in disclosure provisions read into Article 6(3)(b) and (d) ECHR as well as Article 6(1) ECHR, should guarantee the fairness of the trial without the need to resort explicitly to data protection principles. It is not in doubt that the Jersey prosecuting authorities would act in a way that was consistent with Jersey's international human rights treaty obligations. Information concerning the prosecution's case would be made available to the defence, including any exculpatory evidence.

56. As it can be expected that the exemption would be applied in the light of Article 6 and the right to a fair trial, this provision is compatible with the Human Rights (Jersey) Law.

Amendment 8: Amending the provisions relating to the notification fee for charities

57. The draft Amendment Law would allow data controllers whose sole processing activities relate to charity work to be exempt from the notification fee.

58. This provision raises no human rights issues. There is a possibility that others who are required to notify, but have to pay a fee, may argue that they are being discriminated against under Article 14 ECHR read with either the right to respect for private life or property rights. In my view, these arguments would not get off the ground. To rebut them the Jersey authorities could show that you are not comparing

like with like. Alternatively, the difference of treatment can be justified as both necessary and proportionate.

Conclusion

59. Before the Sub-Panel authorises these amendments and before they are put to the States of Jersey, the amendments relating to the exemption of Foundations and the removal of the professional requirements for the President of the Tribunal will need to be reconsidered. The other amendments either are or can be interpreted in a way that is compatible with Jersey's international human rights obligations generally and the Human Rights (Jersey) Law in particular.
60. The advice has reduced the issues to the constitutional protection of international human rights law. It has not sought to engage with other policy considerations; however, those policy considerations can only be debated effectively once it is established that the provisions under discussion comply with Jersey's human rights obligations.
61. If I can be of further assistance in this matter, I would be willing to provide more detailed advice in relation to specific provisions. If new amendments are proposed in relation to data subject access exemptions to Foundations and/or the professional qualification of the tribunal President, I would be pleased to advise further.

Jonathan Cooper OBE
Doughty Street Chambers
16 March 2010

20. APPENDIX 5 – Advocate Helen Ruelle’s Report

Re: The Data Protection Sub-Panel of the States of Jersey (the "Sub-Panel)

Proposed Amendments to the Data Protection (Jersey) Law 2005

BACKGROUND

Mourant du Feu & Jeune has been appointed to provide advice on Jersey law to the Sub-Panel in relation to certain proposed amendments to the Data Protection (Jersey) Law 2005 as amended (the "Law"). This report is a summary of the advice which has been provided by Mourant du Feu & Jeune to the Sub-Panel during the course of its considerations of the proposed amendments to the Law.

Please note that whilst this report comments on certain aspects of the laws of other jurisdictions, as requested by the Sub-Panel, we are not able to offer legal advice in relation to the laws of those jurisdictions.

There are eight proposed amendments to the Law, in summary, as follows:

A proposed increase in the powers of the Data Protection Commissioner (the "Commissioner") to serve information notices ("**Amendment One**");

A proposed amendment to the professional qualifications which the President of the Data Protection Tribunal should hold ("**Amendment Two**");

A proposed increase in the criminal sanctions available on prosecution of an offence under Article 55 of the Law ("**Amendment Three**");

An proposed increase in the powers of seizure under the Law ("**Amendment Four**");

A proposed increase in the charges made to a data subject in relation to health records ("**Amendment Five**");

A proposed amendment relating to the Foundations (Jersey) Law 2009 ("**Amendment Six**");

A proposed amendment to add Article 41 of the Drug Trafficking Offences (Jersey) Law 1988 to the list of exemptions from data subject access requests ("**Amendment Seven**"); and

A proposed waiver of the notification fee for charities ("**Amendment Eight**").

This report will look at each of those proposed amendments in turn.

SUMMARY OF ADVICE

Amendment One - There appears to be a lack of clarity in the Law relating to penalties for breach of Article 47 and it is suggested that this be considered further if Article 43 is to be amended as envisaged by Amendment One. This amendment extends the ambit of the Law beyond data controllers and data processors and gives the Commissioner wide powers. It is, therefore, necessary to assess whether this is a proportionate response bearing in mind the rights of data subjects

under the Law and the limited number of occasions on which such a power may be utilised.

Amendment Two - There appears to be some concern as to whether this amendment is human rights compliant. It is therefore suggested that consideration is given to a requirement that the President of the Tribunal has been qualified as a lawyer for a specified period of time to try and meet those concerns.

Amendment Three - There is a perception that the penalties for offences under the Law may be inconsistent and it is therefore suggested that this issue is considered further.

Amendment Four - It is suggested, if this amendment is adopted, that the Law is reviewed for any further required consequential amendments for example Article 61 relating to the Court's powers to forfeit, destroy or erase.

Amendment Five - No comments from a legal perspective.

Amendment Six - It would appear from the advice of Mr. Jonathan Cooper, OBE that further consideration of the possible human rights implications is required.

Amendment Seven - No comments from a legal perspective.

Amendment Eight - No comments from a legal perspective.

AMENDMENT ONE

This amendment amends Article 43 of the Law. Article 43 currently allows the Commissioner to serve a notice on a data controller or a data processor (ie a custodian of personal data under the Law) requiring that entity to provide certain specified information to the Commissioner. Such a request may be made either if the Commissioner (i) has received a request under Article 42 of the Law (ie a request for an assessment by the Commissioner as to whether certain processing of personal data is or is not being carried out in accordance with the Law); or (ii) reasonably requires information for the purposes of determining whether a data controller has complied with or is complying with the data protection principles.

This amendment would allow the Commissioner to serve an information notice on "any person" (ie not just a data controller or a data processor) in the same circumstances as currently provided by the Law. An information notice may be served on any person whether or not any processing has been carried out by the person on whom the notice is served.

In serving an information notice on "any person", the notice would be required to contain some or all of the following, depending upon the reason for serving the notice:

- a statement that the Commissioner has received a request under Article 42 (if applicable);
- a statement that the Commissioner regards the information specified in the notice as relevant in order to determine whether any processing has been or is being carried out in compliance with the Law;

- the reasons for the Commissioner considering that the specified information is relevant; and
- a statement that the Commissioner reasonably believes that the person on whom the information notice has been served has the specified information.

Anyone on whom an information notice is served has the right of appeal to the Data Protection Tribunal against the notice pursuant to Article 48 of the Law.

Pursuant to Article 47 of the Law, a person who fails to comply with an information notice would be guilty of an offence.

A person may also be guilty of an offence under Article 47 if the person in purported compliance with an information notice either (i) makes a statement that the person knows to be false in a material respect; or (ii) recklessly makes a statement that is false in a material respect.

Pursuant to Article 61 of the Law, a person guilty of an offence under the Law shall, unless the Law provides otherwise, be liable to a fine.

However, in relation to the provision of false information, the provisions of Article 60 of the Law apply. Article 60 provides, in summary, that any person who knowingly or recklessly provides the Commissioner with information that is false or misleading in a material respect shall be guilty of an offence if the information is provided in purported compliance with a requirement imposed under the Law or where the person providing the information intends or could reasonably be expected to know that the information would be used by the Commissioner for the purposes of carrying out the Commissioner's functions under the Law.

There appears, therefore, to be some inconsistency and uncertainty in the penalty that the Court may impose in relation to information notices, for example:

- it is clear that failure to respond to an information notice at all is an offence for which the penalty is a fine;
- however, if an individual were to provide false information in response to an information notice, this appears to be an offence both under Article 47 and Article 60. It would appear to be the case that given the specific reference in Article 47 to offences in relation to providing false information in response to an information notice and that Article 60 is a more general offence, Article 47 would apply in these circumstances. If that is correct, then the penalty would be a fine alone. However, if a prosecution were instead to be brought under the provisions of Article 60, then the penalty would be up to 5 years imprisonment and/or an unlimited fine. It may, of course, be the case that offences in this regard would be committed under both Articles 47 and 60. This, however, leads to a situation where the penalties which may be imposed for essentially the same offence are dramatically different;
- a further difficulty arises in situations where an individual provides misleading information in response to an information notice. In this case, this would not constitute an offence under Article 47 (which only deals with the provision of false information) but it does appear to be caught by the offences set out in Article 60. In this circumstance, therefore, a person may be liable to a term of imprisonment of up to 5 years and an unlimited fine for providing misleading information when under Article 47 read in conjunction with Article 61, the penalty for providing false information, which would appear to be the more serious offence, is a fine alone.

It is suggested that the issues relating to penalties for breach of Article 47 should be considered further if this amendment is to be adopted.

Amendment One - Comments on Drafting

We have no particular comment on the drafting of Amendment One although we do query whether the drafting should make it clear that there should be some reasonable belief on the part of the Commissioner that there is a connection between the data controller who may be in breach and the individual on whom the information notice is served and/or that all other reasonable avenues have been exhausted prior to service of the information notice on a third party.

Comparison with other jurisdictions - UK

It is understood that the UK's Data Protection Act 1998 does not contain a power similar to that proposed by Amendment One.

It is further understood that the UK Information Commissioner has lobbied for an amendment similar to Amendment One to the UK data protection legislation but that, to date, no such amendment has been accepted by the legislature.

In considering the possible reasons for not including this amendment in UK law, the considerations of the House of Commons Standing Committee are noted:

"..... we do not believe it right to give the commissioner power to serve an information notice on a third party..... It is the controller's activities that the commissioner is investigating. It is right that she should be able to require him to provide the information that she needs. However, to extend that to third parties would, in our view, be to give the commissioner an unjustifiably wide power. It would effectively permit her to demand information from anyone at all, whatever their connection to a controller, on threat of criminal sanction. That would be excessive, intensive, and quite inappropriate to a regulatory authority of this nature, however general its remit."

In addition, the UK's Deputy Commissioner has stated to the Sub-Panel that the most pressing reason (but not the only reason) why the UK Information Commissioner has argued for such a power is to enable investigation of breaches of the Privacy and Electronic Communications Regulations 2003 (the "PECR Regulations"). It is understood that these Regulations regulate the processing of personal data and the protection of privacy in the electronic communications sector. There are currently no equivalent statutory provisions in Jersey.

Comparison with other jurisdictions - Guernsey

It is understood that Guernsey has adopted the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance 2004 (the "Ordinance"). The Ordinance, it is understood, replicates the PECR Regulations from the UK.

It is understood that the Data Protection (Bailiwick of Guernsey) (Amendment) Ordinance 2010 (the "Amendment Ordinance") amends the Guernsey Law. The Amendment Ordinance appears, in summary, to extend the Guernsey Commissioner's powers to serve information notices, in certain circumstances, on data processors in addition to data controllers. Prior to the coming into force of the Amendment Ordinance, it is understood that the Guernsey Commissioner was only able to serve an information notice on a data controller.

According to the States of Guernsey official website (<http://www.gov.gg/ccm/home-department/data-protection/news/amendments-to-the-law.en>), with effect from 1 March 2010, Guernsey law has been amended to allow the service of information notices concerned with alleged breaches of electronic communications regulations on any person (although the author of this report has been unable to locate the amending provision to the Guernsey Law which effects this).

Therefore, it appears that in Guernsey, the power to serve information notices on any person only extends to alleged breaches of the electronic communications regulations, which the author takes to mean the Ordinance or subordinate legislation thereunder.

Comparison with other jurisdictions - Ireland

It is understood that data protection legislation in Ireland allows the service of an information notice on any person.

Issues

The author believes that the extract above from the House of Commons Standing Committee debate reflects many of the issues highlighted by the Sub-Panel in considering this proposed amendment:

Data protection legislation is enacted to place direct obligations upon custodians of personal data and to give rights to those whose data is processed by a data controller or data processor. The Law does not place obligations on anyone other than a data controller/processor. This amendment would extend the ambit of data protection legislation beyond the relationship between data controller and data subject;

Evidence from both the Commissioner in Jersey (supported by evidence received from the Assistant Commissioner in Ireland) suggest that the number of circumstances in which such a power may actually be required is very limited;

That said, of course, the fact that a power may only be invoked in limited circumstances, does not, in itself, mean that it is not required. Indeed, the Law does not only place obligations on data controllers; it gives rights to data subjects. The evidence of the Commissioner states that on occasion, she has been unable to fully investigate whether an individual's rights under the Law have been breached because of an inability to require a third party to provide information. The Commissioner was keen to stress that in these types of cases, there is often no "fault" on the part of the third party - the request is merely one of information which would then allows the Commissioner to assess to what extent there has been a breach by a data controller;

Article 55 of the Law already provides a course of action in some circumstances. Article 55 states that a person who knowingly or recklessly without the consent of the relevant data controller (i) obtains or discloses personal data; or (ii) procures the disclosure of personal data shall be guilty of an offence for which the current penalty is a fine. Therefore, in some circumstances, there is an ability for the Commissioner to involve the police in an investigation where it is considered that an Article 55 offence has been committed;

There was a concern expressed in evidence before the Sub-Panel that given the increased use in technology and other developments, the possibility of very serious breaches of data protection legislation is increased;

Evidence was received from the Commissioner that there have been a very limited number of circumstances where she has not been able to pursue alleged serious breaches of the Law because of an inability to require information from other than a data controller;

The issue therefore appears to be one of proportionality - ie is it proportional to extend the ambit of the Law to require information from third parties given the low number of instances in which this power has, to date, been required and bearing in mind

- (i) the existing offence under Article 55;
- (ii) that failure to comply with an information notice would be a criminal offence;
- (iii) that the Law currently only places obligations on data controllers and data processors; and
- (iv) that without such powers the rights of data subjects may not be enforced.

AMENDMENT TWO

This amendment amends Schedule 5 of the Law to remove the requirement for the President of Data Protection Tribunal to be an advocate or solicitor of at least 7 years' standing. The individual appointed would, however, still be required to be a Jersey qualified advocate or solicitor.

Amendment Two - Comments on Drafting

We have no particular comment on the drafting of Amendment Two.

Comparison with other jurisdictions - UK

It is understood that in order to be appointed President of the equivalent Tribunal in the UK, the individual must have seven years general qualification.

Issues

It has been highlighted by Mr Jonathan Cooper in his advice to the Sub-Panel on the human rights implications of the proposed amendments that this proposed amendment may not be human rights compliant and the author reads that advice with interest.

Jersey is a slightly different jurisdiction from others in terms of legal advisers. It can be the case that a very senior lawyer who, for example, has had a significant number of years' experience in another jurisdiction has only recently qualified as a Jersey advocate or solicitor. It is believed that this amendment would allow such a person, who indeed may be very highly qualified in this area or in the law generally to be considered for the role. Conversely, the proposed wording of Amendment Two would mean that a very junior lawyer who is only recently qualified in Jersey and with no experience in any other jurisdiction could, theoretically, be appointed to the role (although the author queries whether in practice this would be the case.)

The author wonders if in order to meet some of the concerns of Mr Jonathan Cooper, consideration should be given to requiring that the President be qualified for a specified number of years as a lawyer but that such a period of qualification need not be as a Jersey advocate or solicitor? It is noted that Amendment Two requires the President to be a Jersey qualified advocate or solicitor and therefore any such requirement could be in addition to this. It is also noted that pursuant to the Employment Tribunal (Jersey) Regulations 2005, the Chairman and the Deputy Chairman of that tribunal are required to hold a "qualification in law". This is not defined and therefore does not restrict the holder of the post to a certain number of years' qualification or to being a Jersey qualified lawyer.

AMENDMENT THREE

This amendment amends Article 55 of the Law to provide that a person guilty of an offence under Article 55 shall be liable to a term of imprisonment of two years and a fine.

Article 55 of the Law currently states that a person who knowingly or recklessly without the consent of the relevant data controller (i) obtains or discloses personal data; or (ii) procures the disclosure of personal data shall be guilty of an offence. Pursuant to the provisions of Article 61 of the Law, currently, a person guilty of an offence under Article 55 of the Law shall be liable to a fine.

Amendment Three - Comments on Drafting

We have no particular comment on the drafting of Amendment Three.

Comparison with other jurisdictions - UK

It is understood that this amendment mirrors an amendment to the UK law which is due to come into force during the course of 2010 albeit that there are some exemptions in relation to journalistic activity which are not reflected in the Jersey law - see further below.

Issues

Criminal offences

The current penalty under the Law is a fine. Article 13 (2) of the Interpretation (Jersey) Law 1954 provides that "*where a penalty for an offence is a fine and the amount of the fine or a level on the standard scale is not specified, the fine shall be construed as a fine of an unlimited amount.*"

It is also clear that by virtue of Article 13 (3) of the Interpretation (Jersey) Law 1954 the words "and a fine" mean, in practice, that the Court may, on conviction, impose a term of imprisonment and/or a fine i.e. the penalties may be imposed alternatively or cumulatively.

Amendment Three therefore would increase the penalty available for conviction of an Article 55 offence to include a term of imprisonment of up to two years. The fine would be unlimited.

It is noted that for other offences under the Law (for example the offences under Article 60 discussed above) that the penalty is up to 5 years' imprisonment and an unlimited fine. Therefore, the penalty for providing false or misleading information to the Commissioner, for example, could attract a significantly longer term of imprisonment than, for example, a deliberate, unlawful disclosure of personal data (e.g. sale of a database for a significant sum) where the maximum term of imprisonment would be 2 years.

It is, therefore, suggested that the offences under the Law be further considered to ensure that the penalties are consistent with each other in light of the proposed amendments to the Law.

Other legislation

The Sub-Panel heard and received evidence that the Law is looked to for sanctions and penalties in relation to other legislation such as the Sex Offenders (Jersey) Law 2010 - in particular, the Sub-Panel was made aware of the importance of this amendment by the Minister for Home Affairs.

There is also evidence to suggest that this amendment would bring the Law in line with other pieces of legislation such as the Financial Services (Jersey) Law 1998 and Banking (Depositors Compensation) (Amendment) (Jersey) Regulations 2010.

"Reasonable Belief"

It is understood that in the UK a similar amendment to Amendment Three is expected to come into force during the course of 2010. It is also understood that there has been concern in the UK that this amendment may have an adverse effect on journalism. As a result, a defence has been added to the UK Act to the effect that where there is a reasonable belief that the obtaining, disclosing or procuring of the information was justified as being in the public interest, an offence under Article 55 would not have been committed.

Article 55 of the Law currently provides that a person will not commit an offence if the person can show that "in the circumstances of the case, the obtaining, disclosing or procuring was justified as being in the public interest." There is no equivalent of the "reasonable belief" text.

AMENDMENT FOUR

This amendment amends Schedule 9 of the Law by adding a direct reference to the ability of the Commissioner, with a warrant, to seize not only documents and other material but also equipment.

It also seeks to correct an omission in the Law. Paragraph 14 of Schedule 9 is entitled "Power to Require Information". However, the text of paragraph 14 currently only refers to a power for the Commissioner to request documents when investigating an offence and not information. The amendment, therefore, includes an ability to request documents and information in such circumstances.

Amendment Four - Comments on Drafting

We have no particular comment on the drafting of Amendment Four.

Comparison with other jurisdictions - UK

It is understood that the amendment relating to the addition of "equipment" does not form part of UK law.

Issues

Schedule 9 as drafted is arguably ambiguous. The provisions of Schedule 9 provide that once a warrant has been obtained by the Commissioner from the Bailiff or a Jurat, the Commissioner's staff may enter premises for the following purposes:

- To search those premises
- To inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data
- To inspect and seize and documents or other material found there

On one reading of the Law, as drafted, there is some concern that given that equipment is mentioned only in the context of inspection, examination, operation and testing, the power to seize may not extend to equipment.

There is also, however, a suggestion that the power to seize "other materials" may extend to a power to seize equipment. However, there is a lack of certainty in this regard. The Sub-

Panel heard evidence from the Commissioner that this lack of certainty is a concern especially given that much personal data is today stored and processed electronically.

It does, therefore, seem to be the case that this is a possible loophole which, for the sake of certainty and clarity, should be closed.

There was some concern expressed to the Sub-Panel about the impact which seizing equipment, such as computers, may have on a business's ability to operate. However, the Commissioner gave evidence that such seizures are conducted in conjunction with the police and that, whilst there may be some disruption, this would be kept to a minimum bearing in mind that the breach of the Law must have been particularly serious for the Commissioner to have obtained a warrant to seize equipment in the first instance. In these cases, the granting of a warrant is by the Bailiff or a Jurat subject to certain safeguards.

It has also been highlighted that if this amendment is adopted, it would be prudent to ensure that the Law is consistent throughout in the use of the words "document, equipment and other material". For example, in Article 61, the Court's powers to forfeit, destroy or erase on conviction of certain offences only apply to "any document or other material used in connection with the processing of personal data."

AMENDMENT FIVE

This amendment amends to Data Protection (Subject Access Miscellaneous) (Amendment) (Jersey) Regulations 2005 (the "Regulations") to increase the maximum fee which may be charged in respect of a data subject access request from £10 to £50 where that request relates wholly or mainly to personal data forming part of a health record.

Under the Law, such subject access requests were the subject of a maximum £50 fee for a transitional period which ended in 2008. Currently, therefore, the maximum fee which it is possible to charge for such data subject access requests is £10 which is the same maximum charge for all other data subject access requests.

Amendment Five - Comments on Drafting

We have no particular comment on the drafting of Amendment Five.

Comparison with other jurisdictions - UK

It is understood that in the UK there is a maximum charge in respect of data subject access requests relating to health records of £50.

Issues

It was thought that there may be some concern expressed by other data controllers that a maximum charge of £50 only relates to health records especially whether other data controllers are required to provide complex data on a data subject access request (such as CCTV footage or telephone conversations). However, evidence given by the Chamber of Commerce appears to suggest that this is not a concern for Chamber members.

It is also noted that this amendment may be considered to be a deterrent for some, given the cost of exercising their right under the Law to make a data subject access request.

It is noted that whilst the Regulations provide that the maximum fee is £50, there is no provision in either Law or the Regulations which regulate how a data controller should calculate the fee which may be charged, up to the maximum amount. However, it is considered that such a provision would be complex to draft and is not applicable only to the

fee relating to health records. In addition, evidence from the Minister for Health & Social Services and the Information Governance Manager of Health & Social Services made it clear that discretion is exercised in determining the appropriate fee up to the maximum level and that this discretionary application had been in place, in practice, during the transitional period of the Law.

AMENDMENT SIX

This amendment exempts from the subject access provisions of the Law, personal data in respect of a foundation. It mirrors a similar provision which is already in force in respect of personal data in respect of a trust.

The Foundations (Jersey) Law 2009 (the "Foundations Law") provides that except as specifically required by or under the Foundations Law or by the charter or regulations of the foundation, a foundation is not required to provide any person (whether or not a beneficiary) with any information about the foundation. In particular, information about:-

- (a) the administration of the foundation;
- (b) the manner in which its assets are being administered;
- (c) its assets; and
- (d) the way in which it is carrying out its objects.

That, of course, is without prejudice to any other obligation of a foundation to supply any information about the foundation imposed by an enactment or by an order of the court. An example of the latter may occur where a beneficiary has become entitled to a benefit in accordance with the charter or the regulations and the benefit is not provided.

The advice of Mr Cooper is noted in this regard. However, it would appear that to permit a data subject access request relating to personal data in respect of a foundation would be in direct conflict with the provisions of the Foundations Law. It should also be noted that a similar wholesale exemption is available in respect of trusts.

Amendment Six - Comments on Drafting

We have no particular comment on the drafting of Amendment Six.

AMENDMENT SEVEN

This amendment amends the Data Protection (Subject Access Exemptions) (Jersey) Regulations 2005 to exempt from the data subject access request provisions of the Law personal data which would otherwise be prohibited or restricted by virtue of Article 41 of the Drug Trafficking Offences (Jersey) Law 1988 (the "Drug Trafficking Law"). This article relates to "tipping off" offences.

Amendment Seven - Comments on Drafting

We have no particular comment on the drafting of Amendment Seven.

Issues

This amendment appears to be suggested because of an oversight in the original Law and is, in our view, uncontroversial. The amendment seeks to close a loophole whereby the Drug

Trafficking Law prohibits certain disclosures but the Law would require that information to be disclosed as part of a data subject access request.

AMENDMENT EIGHT

This amendment amends the Data Protection (Notification) (Jersey) Regulations 2005 relating to the fee to be charged to certain organisations as data controllers for inclusion in the register of data controllers. It is a statutory obligation for data controllers to notify the Commissioner that they are data controllers and to provide certain prescribed information in respect of that notification. The current fee for notification is £50.

The amendment states that any corporation, association, trust or non-profit organisation exempt from income tax under certain provisions of the Income Tax (Jersey) Law 1961 are not required to pay the £50 notification fee except where notification is made in the name of a school. In practice, this exempts, charities, broadly speaking.

Amendment Eight - Comments on Drafting

We have no particular comment on the drafting of Amendment eight.

Issues

This appears to be an uncontroversial amendment and therefore we have no particular comment from a legal perspective.

Mourant du Feu & Jeune
March 2010

21. APPENDIX 6 – Minister for Economic Development: Letter 23rd March 2010

Economic Development Department

Liberation Place
St Helier, Jersey, JE1 1BB
Tel: +44 (0)1534 448886
Fax: +44 (0)1534 448171



Deputy T Vallois
Chairman, Corporate Services Data Protection Sub-Panel
Scrutiny Office
Morier House
Halkett Place
St Helier
Jersey JE1 1DD

23 March 2010


Dear Deputy Vallois

Further to my letter dated 03 March 2010, officers from the Economic Development Department ("the Department") have now had the opportunity of discussing the proposed amendments to the Data Protection (Jersey) Law 2005 ("the Law") with the Data Commissioner and I am therefore writing to update the Corporate Services Scrutiny Sub-Panel ("the Sub-Panel") in this regard.

In relation to the concern I raised previously with regard to the proposed extension of the powers of the Data Protection Commissioner ("the Commissioner") to issue information notices to persons other than data controllers, having discussed this matter with the Commissioner, the Department is persuaded that in the light of the fact that only a few notices are issued each year, the proposed extension is an appropriate means of dealing with the enforcement and compliance issues currently facing the Commissioner in this regard and should not have a serious affect on businesses in Jersey. On that basis, the Department does not oppose the proposed extension of the Commissioner's power under Article 43.

Although the Department was initially concerned about the extent of the seizure powers of the Commissioner, in particular with regard to the power to retain seized material for 'as long as is necessary', having carried out a comparative analysis, the Department is satisfied that the extent of this provision is commensurate with the corresponding seizure powers of the States of Jersey Police (as set out in Police Procedures and Criminal Evidence (Jersey) Law 2003) and the UK Data Commissioner (as set out in Data Protection Act 1998).

Further, having discussed the other proposed amendments to the Law in the context of the issues facing the Commissioner and having received assurances with regard to the proposed safeguards, the Department does not object to the proposed amendments to the Law.

Please let me know if I can be of any further assistance.

Yours sincerely



Senator Alan Maclean
Minister for Economic Development

22. APPENDIX 7 – Minister for Economic Development: Letter 3rd March 2010

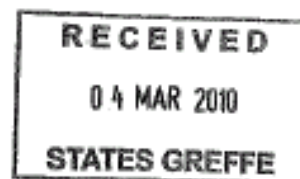
Economic Development Department

Liberation Place,
St Helier, Jersey, JE1 1BB
Tel: +44 (0)1534 448886
Fax: +44 (0)1534 448171



Deputy T Vallois
Chairman, Corporate Services Data Protection Sub-Panel
Scrutiny Office
Morier House
Halkett Place
St Helier
Jersey JE1 1DD

03 March 2010



Dear Deputy Vallois

Thank you for your letter dated 23 February 2010 regarding the review of the Corporate Services Scrutiny Sub-Panel (**"the Sub-Panel"**) into the proposed amendments to the Data Protection (Jersey) Law 2005 (**"the Law"**).

I appreciated the opportunity of attending the Public Hearing on 19 February 2010 to discuss how the proposed amendments might affect the business community in Jersey. Further to your letter, I am enclosing a copy of a letter from Jersey Finance setting out some of the concerns its members regarding the proposed amendments.

In addition to the matters set out in the enclosed letter, you may recall that during the course of the Public Hearing, I expressed some concern with regard to the fact that the proposed amendment to Article 43 of the Law would extend the powers of the Data Protection Commissioner (**"the Commissioner"**) beyond those that apply, for example, in the United Kingdom.

Having looked into the matter further, I remain unconvinced of the need to extend the Commissioner's power in relation to information notices so that such notices may be served on a person other than data controller (or data processor). Although it is right to say, as the Commissioner's Report does, that the analogous UK authority has asked for an equivalent power for its Commissioner, it is noteworthy that this suggestion has never been taken up by UK legislators and, notably, was not taken up during the development of the recent Coroners and Justice Act 2009.

It is also interesting to note that the case put forward by the UK Information Commissioner for such an 'Extended Information Notice Power' appears to have been based primarily on the need to address concerns in relation investigations concerning Privacy and Electronic Communications (**"PECR"**) breaches, where it is apparently often necessary to identify who the subscriber to a particular phone or fax number is, or who is 'behind' an e-mail address or website – see highlighted passage enclosed.

Although the Commissioner's Report states that difficulties have been encountered in obtaining information in the course of investigations, no details are provided and I am not aware that PECR breaches are of particular concern in Jersey. I would therefore question the need for the Commissioner to have the extended powers that were requested, but ultimately not granted, in the United Kingdom. It may be that the Commissioner is able to provide more supporting evidence of the need for this extended power, but I would suggest that this should be an area of further interest in the Sub-Panel's review of the proposed amendments to the Law.

Please let me know if I can be of any further assistance.

Yours sincerely



Senator Alan Maclean
Minister for Economic Development