DATA PROTECTION PRACTICAL APPLICATION (GUERNSEY) UNIT - SYLLABUS

ELEMENT 1 – INTRODUCTION TO THE DATA PROTECTION CULTURE

1.1 – GLOBAL SHIFT IN CULTURE

The candidate should:

1.1.1	understand why the requirements for data protection have changed over time
1.1.2	understand that changes to data protection reach further than Europe
1.1.3	understand equivalency of data protection regimes
1.1.4	know what routes may be used to pass data to processors in non-equivalent jurisdictions

1.2 – CHANGING GUERNSEY'S DATA PROTECTION CULTURE

The candidate should:

1.2.1	know that the Guernsey Law exists distinct from the EU GDPR
1.2.2	understand key differences between the Guernsey Law and the EU GDPR
1.2.3	understand why EU equivalency matters to Guernsey

1.3 – DATA PROTECTION IN BUSINESSES & ORGANISATIONS

The candidate should:

1.3.1	know that a Data Controller or Data Processor can be a legal or natural person
1.3.2	know that a Data Controller or Data Processor can be any type of organisation
1.3.3	understand the role that a board of directors (or other governing body) plays in setting the data protection culture of an organisation
1.3.4	understand the role that a board of directors (or other governing body) plays in setting appropriate policies for an organisation
1.3.5	understand that the policies or an organisation should drive the procedures and processes of the organisation
1.3.6	understand that there is a role for every individual in the organisation in respect of data protection

1.4 – DATA PROTECTION & RETENTION POLICIES

The candidate should:

1.4.1	understand the purpose of a data protection policy
1.4.2	know the standard contents of a data protection policy
1.4.3	understand the purpose of a data retention policy
1.4.4	understand that a data retention policy may need to take into account other laws and regulations
1.4.5	understand the role that an information security policy or a cyber security policy may play in data protection

ELEMENT 2 – IDENTIFICATION & USAGE OF PERSONAL DATA

2.1 – DEFINING PERSONAL DATA AND SPECIAL CATEGORY DATA

The candidate should:

2.1.1 know what personal data and special category data are

2.1.2 understand the differences when dealing with special category data

2.2 – IDENTIFYING WHERE PERSONAL DATA IS STORED

The candidate should:

2.2.1 know the various media and applications that can be used to store personal data

2.2.2 understand the vulnerabilities associated with hard copy data

2.2.3 understand the vulnerabilities associated with electronically stored data

2.2.4 understand the difficulties posed when individuals store data outside approved systems and databases

2.3 – ASCERTAINING WHAT PERSONAL DATA IS USED FOR

The candidate should:

2.3.1 know that all personal data collected should have legitimate use connected with the services an organisation provides to its clients/users

2.3.2 understand the processes an organisation should have in place to identify usage of personal data

2.3.3 know that data not being used for a specific purpose should not be held

2.4 – MAINTAINING & ACCESSING PERSONAL DATA

The candidate should:

2.4.1 understand that for data to be of use it should be accessible

2.4.2 understand that for data to remain up to date it should be maintained

2.4.3 understand that controls should be in place for access of data to ensure data is not accessed by someone not authorised

2.4.4 understand that controls should be in place for maintenance of data to ensure that it is not incorrectly amended

2.5 – PERFORMING A DATA AUDIT

The candidate should:

2.5.1 know what a data audit is

2.5.2 understand the role that a data audit plays in identifying data held and its uses

2.5.3 understand the role that a data audit plays in providing the board with appropriate information to set policies

2.5.4 understand the role that a data audit plays in identifying multiple instances of data and possible inconsistencies between those instances

2.5.5 understand the role data a data audit plays in identifying data held without purpose

2.6 – PERFORMING A PRIVACY IMPACT ASSESSMENT

	The candidate should:
2.6.1	know what a Privacy Impact Assessment is
2.6.2	understand what factors should be taken into account for the Privacy Impact Assessment
2.6.3	understand how a Privacy Impact Assessment can inform an organisation about the risks involved in processing its data
2.6.4	understand the role that a Privacy Impact Assessment plays in providing the board with appropriate information to set policies
2.6.5	understand how a Privacy Impact Assessment can be used to reduce risks in processing data

2.7 – HIGH RISK SITUATIONS

	The candidate should:
2.7.1	know that where a Privacy Impact Assessment identifies a high risk in processing data permission should be sought from the Data Protection Commissioner in respect of that processing
2.7.2	understand that where a Privacy Impact Assessment identifies a high risk in processing data the organisation should firstly seek to reduce the risk by putting appropriate controls in place

2.8 – MISUSE OF DATA

	The candidate should:
2.8.1	know that data should be collected for specific purposes only
2.8.2	understand that misuse of data can be for apparently legitimate in the context of the organisation
2.8.3	understand that misuse of data can result from inadvertent or malicious action from within an organisation

2.9 – FINDING A BALANCE – KNOW YOUR CLIENT VS KNOWING TOO MUCH

	The candidate should:
2.9.1	know that in some types of businesses there are reasons to hold personal data in order to establish the business relationship
2.9.2	understand that proportionality needs to be achieved in balancing the requirement to understand the nature of a business relationship and the identity of a customer against holding excessive amounts of data

ELEMENT 3 – IMPLEMENTING AFFIRMATIVE CONSENT

3.1 – AFFIRMATIVE CONSENT VS PASSIVE CONSENT

The candidate should:

3.1.1	know what is meant by affirmative consent
3.1.2	know what is meant by passive consent
3.1.3	understand the differences between affirmative consent and passive consent
3.1.4	know that under the revised data protection framework there is a requirement to move from passive consent to active consent
3.1.5	understand that consent may need to be re-obtained

3.2 – CHANGES TO FORMS – PHYSICAL AND ONLINE

The candidate should:

3.2.1	understand how active consent can be achieved using a physical form
3.2.2	understand how active consent can be achieved using an online form

3.3 – CONSENT FOR GIVEN PURPOSES

The candidate should:

3.3.1	know that consent must relate to given purposes in respect of the business relationship between the client and the organisation
3.3.2	know that where the business relationship requires additional purposes to processing of data that new consent must be obtained
3.3.3	understand that where consent has been obtained for specified purposes it cannot be assumed for other purposes

3.4 – CONSENT FOR MINORS

The candidate should:

3.4.1	know the age of minority under data protection legislation
3.4.2	know that consent in respect of a minor must be received from an adult responsible for that minor

3.5 – TERMS AND CONDITIONS; PRIVACY POLICY

The candidate should:

3.5.1	know what Terms and Conditions are
3.5.2	know what should be contained within Terms and Conditions for data protection purposes
3.5.3	know what a Privacy Policy is
3.5.4	know what should be contained within a Privacy Policy for data protection purposes

ELEMENT 4 – ENSURING THE RIGHTS OF THE DATA SUBJECT

4.1 – DEALING WITH SUBJECT ACCESS REQUESTS

	The candidate should:
4.1.1	know what a Subject Access Request is
4.1.2	know what timeframes a Subject Access Request should be completed within
4.1.3	understand what should be done to comply with a Subject Access Request
4.1.4	know what data may be excluded from a Subject Access Request

4.2 – DEALING WITH DATA PORTABILITY

	The candidate should:
4.2.1	understand what Data Portability is
4.2.2	know the parameters within which Data Portability operates
4.2.3	understand that the Data Audit can be used to assist with identifying data sources to be used for Data Portability

4.3 – DEALING WITH INCORRECT DATA

	The candidate should:
4.3.1	understand that data integrity is important for the organisation
4.3.2	understand that incorrectly maintained data can result in a data breach
4.3.3	know that a data subject has the right to have their data rectified
4.3.4	understand that incorrectly maintained data can be classified as a data breach

4.4 - RIGHT TO ERASURE – A LIMITED RIGHT

	The candidate should:
4.4.1	know that there is the Right to Erasure
4.4.2	understand the limitations to the Right to Erasure

4.5 – RIGHTS RESTRICTING PROCESSING & AUTOMATED DECISION MAKING

	The candidate should:
4.5.1	know that a data subject has the right to restrict processing of their data
4.5.2	know that a data subject has the right not to have automated decision making processed on their data
4.5.3	understand what an organisation needs to do to comply with both of these rights

4.6 – RIGHT TO OBJECT

	The candidate should:
4.6.1	know that a data subject has the right to object to their data being processed
4.6.2	understand that an organisation needs to do to comply with the Right to Object

4.7 – RESTRICTIONS TO RIGHTS

	The candidate should:
4.7.1	know that there are restrictions to the rights of a data subject
4.7.2	know what the restrictions to the rights of a data subject are

ELEMENT 5 – DEALING WITH DATA PROTECTION BREACHES

5.1 – IDENTIFICATION OF A BREACH

The candidate should:

5.1.1	understand that a breach may occur some time before it is identified
5.1.2	understand that the point of identification of a breach is the base of the breach handling timeline
5.1.3	understand that an organisation may be expected to have reasonable measures in place to assist in identification of a breach
5.1.4	understand that some breaches may be identified by parties outside the organisation

5.2 – INTERNAL BREACH PROCESSES

The candidate should:

5.2.1	understand the importance in an organisation having clear processes for dealing with a breach
5.2.2	understand that a breach process should assign responsibility to individuals or teams within a business
5.2.3	understand that a breach can be used as a learning experience so that an organisation can put measures in place to mitigate future breaches

5.3 – REPORTING TO REGULATOR

The candidate should:

5.3.1	know that reporting of data protection breaches is mandatory
5.3.2	know the maximum timescale within which a breach must be reported
5.3.3	know the minimum information that must be provided to the regulator in the breach report
5.3.4	know that an individual should be identified as the contact point for the regulator
5.3.5	understand that breach reporting should be kept factual and to the relevant points only
5.3.6	know the sanctions that may be imposed

5.4 – REPORTING TO DATA SUBJECTS

The candidate should:

5.4.1	know that there are some circumstances where a data breach may need to be reported to the affected data subjected
5.4.2	understand that this is an opportunity for the organisation to control the message and ensure that appropriate assurances are made
5.4.3	understand that data subjects will be reassured if additional measures are put in place to prevent recurrence

5.5 – DEALING WITH THE MEDIA

The candidate should:

5.5.1	understand that in some circumstances the media may be made aware of a data breach
5.5.2	understand that this can come from official sources or disgruntled clients
5.5.3	understand that the organisation needs to have a clear message prepared including details of any mitigating factors or controls put in place

ELEMENT 6 – ROLE OF THE DATA PROTECTION OFFICER (DPO)

6.1 – IS A DATA PROTECTION OFFICER NECESSARY

A candidate should:

6.1.1	know the circumstances in which a DPO is mandatory
6.1.2	understand that any organisation where a DPO is not mandatory may still choose to appoint one
6.1.3	understand why an organisation may not wish to appoint a DPO

6.2 – THE "DE FACTO" DATA PROTECTION OFFICER

A candidate should:

6.2.1	understand that if an individual is fulfilling the functions of the DPO they can be classified as a DPO without being formally allocated the title
6.2.2	understand that where the functions of a DPO are split between various individuals none of them can be individually identified as fulfilling the DPO function

6.2 – THE "DE FACTO" DATA PROTECTION OFFICER

A candidate should:

6.2.1	understand that if an individual is fulfilling the functions of the DPO they can be classified as a DPO without being formally allocated the title
6.2.2	understand that where the functions of a DPO are split between various individuals none of them can be individually identified as fulfilling the DPO function

6.3 – THE DPO – INDEPENDENT AND UNCONFLICTED

A candidate should:

6.3.1	know that whilst a DPO is within the structure of an organisation they may not receive instructions that contradict the nature or function of their role as DPO
6.3.2	know that whilst a DPO can fulfil other duties they must not have duties that conflict with their role as DPO
6.3.3	understand how conflicts can arise and how little scope there can be for other duties
6.3.4	understand that a DPO may have to undertake tasks in direct contravention to the wishes of the board of directors (or other governing body) of the organisation

6.4 – DUTIES OF THE DPO

A candidate should:

6.4.1	know the duties of a DPO
6.4.2	understand the responsibilities of the DPO
6.4.3	understand the requirement for a DPO to report to the regulator
6.4.4	understand that whilst undertaking duties can be assigned responsibility cannot
6.4.5	understand some of the areas where duties can be allocated to other inside or outside the organisation

ELEMENT 7 – INTERFACING WITH DATA PROTECTION REGULATORS

7.1 – OFFICE OF THE DATA PROTECTION COMMISSIONER (DPC)

The candidate should:

7.1.1 know that the Data Protection Commissioner is the regulator for Data Protection in Guernsey

7.1.2 know that the Office of the Data Protection Commissioner is an independent body

7.1.3 understand the role of the Data Protection Commissioner under the Law

7.2 – ORGANISATION & DPC – THE WORKING RELATIONSHIP

The candidate should:

7.2.1 know that the Law requires Organisations to communicate openly with the DPC

7.2.2 know the events that would require an Organisation to contact or report to the DPC

7.2.3 understand how an open working relationship with the regulator can be beneficial to an organisation

Specification last updated: Tuesday, 06 February 2018