2.11 Module 16 Privacy and Data Protection Law

2.11.1 Headline information about the module

Module title	Privacy and Data Protection Law
Module NFQ level (only if an NFQ level can be demonstrated)	N/A
Module number/reference	Module 16
Parent programme(s) the plural arises if there are embedded programmes to be validated.	LLB (Hons)
Stage of parent programme	2
Semester (semester1/semester2 if applicable)	Semester 1 or Semester 2
Module credit units (FET/HET/ECTS)	ECTS
Module credit number of units	5
List the teaching and learning modes	Full Time, Part Time
Entry requirements (statement of knowledge, skill and competence)	Learners to have successfully completed Stage 1 of the programme
Pre-requisite module titles	None
Co-requisite module titles	None
Is this a capstone module? (Yes or No)	No
Specification of the qualifications (academic, pedagogical and professional/occupational) and experience required of staff (staff includes workplace personnel who are responsible for learners such as apprentices, trainees and learners in clinical placements)	Lecturers are expected to hold at least a level 8 legal qualification, preferably with a professional legal qualification and specific practical expertise in the area of data protection and e-Privacy. It is an advantage to have completed the Certificate in Training and Education provided by Griffith College. Preference will be given to Lecturers who can demonstrate practical qualifications in Privacy from reputable organisations such as the IAPP.
Maximum number of learners per centre (or instance of the module)	60
Duration of the module	One Semester, 12 weeks
Average (over the duration of the module) of the contact hours per week	2
Module-specific physical resources and support required per centre (or instance of the module)	Lecture room with internet access and digital projector.

Analysis of required learning effort										
Effort while in contact with staff										
Classroom and demonstrations		**Mentoring and small-group tutoring**		**Other (specify)**		**Directed e-learning (hours)**	**Independent learning (hours)**	**Other hours (specify)**	**Work-based learning hours of learning effort**	**Total effort (hours)**
Hours	**Minimum ratio teacher/learner**	**Hours**	**Minimum ratio teacher/learner**	**Hours**	**Minimum ratio teacher/learner**					
24	1:60						101			125
Allocation of marks (within the module)										
				Continuous assessment		**Supervised project**	**Proctored practical examination**	**Proctored written examination**	**Total**	
Percentage contribution								100	**100%**	

2.11.2 Module aims and objectives

The Module covers a key area of specialized legal knowledge with significant importance for the operation of commercial and non-commercial organisations, both conventional and online, across the European Union. The Module aims to provide learners with a focused knowledge of privacy and data protection law with a particular emphasis on the General Data Protection Regulation. Learners are enabled to understand the importance, scope and hierarchy of privacy and data protection requirements, including the concept of consent and the scope of the remedies and penalties for non-compliance. The Module builds upon this knowledge by enabling learners to understand, examine and apply the protective, administrative practices necessary to comply with the law. Finally, learners are enabled to apply their learning to address a wide range of practical issues and to offer solutions to hypothetical, factual scenarios.

2.11.3 Minimum intended module learning outcomes

On successful completion of this module, learners will be able to:

(i) Communicate a clear understanding of privacy and data protection laws and how they operate;
(ii) Discuss and apply domestic and European law in relation to both privacy and data protection;
(iii) Critique the rights afforded to the individual, including the scope and meaning of consent;
(iv) Analyse the effects of the GDPR in relation to the handling of data, including the enforcement mechanisms and remedies available;
(v) Investigate and evaluate the processes involved in data protection;
(vi) Conduct effective and efficient research on issues related to Privacy and Data Protection Law; and
(vii) Analyse factual problems in light of privacy and data protection law.

2.11.4 Rationale for inclusion of the module in the programme and its contribution to the overall MIPLOs

As a result of the General Data Protection Regulation 2016/679, Data Protection Act 2018 and privacy laws learners should become familiar with the legislation, principles and requirements relating to the area of privacy and data protection within Ireland. This module serves to directly underpin programme learning outcomes 1, 2, 4, 5, 6, 10.

2.11.5 Information provided to learners about the module

Learners will receive the following resources and materials in advance of commencement:

- Module descriptor with module learning outcomes
- Class plan
- Assignment and project brief with assessment strategy
- Reading materials
- Notes

Additionally, this material will be made available through Moodle, the College Virtual Learning Environment, along with other relevant resources and activities.

2.11.6 Module content, organisation and structure

Privacy and Data Protection Law is a 5 ECTS credit module taught and assessed over 12 weeks. The module is delivered over 12 lecture sessions of 2 hours' duration for learners.

The Learning Outcomes for this programme have been aligned with the knowledge, skills and competencies indicated as appropriate for Level 8 on the NFQ. They have been articulated using the *Quality and Qualifications Ireland (QQI) Awards Standards for Honours Bachelor of Laws and Master of Laws (July 2014) and for Generic Higher Education and Training (July 2014)*.

Privacy

- What is privacy?
- Privacy and confidentiality
- History and context of privacy rights

Sources of Privacy Rights

- The inviolability of the Dwelling and Article 40.5.5 of the Constitution of Ireland 1937
- European Convention on Human Rights
- The European Union Charter of Fundamental Rights
- Privacy as a Common Law Right
- Statutory Rights to Privacy
    - *Limited Rights in specific pieces of legislation*
    - *Data Protection Acts 1988/2003*
    - *S10 Non-Fatal Offences against the Person Act 1997*
    - *S114 CRRA 2000*
    - *Mental Health Act 2001*
    - *Adoption Act 2008*
    - *Directive 2002/58/EC – Electronic Privacy Directive*
    - *Directive 2009/136/EC – Cookies Directive*
    - *Directive 2006/24/EC (Communications (Retention of Data) Act 2011)*
    - *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*
    - *Criminal Justice (Surveillance) Act 2009*
    - *Privacy Bill 2012*
    - *EU E-Privacy Regulation on the Respect for private life and the protection*
    - *Personal data in electronic communications (repealing Directive 2002/58/EC)*
- Spam
- Value of Privacy Rights (Case Law)
- Penalties and Remedies for Breach of Privacy
    - *Criminal Law*
    - *Civil Law*

Data Protection

- Data Protection Legislation
    - Data Protection Act 1988
    - Data Protection Directive 1995 - Directive 95/46/EC
    - Data Protection (Amendment) Act 2003
    - General Data Protection Regulation 2016
    - Data Protection Act 2018

- General Data Protection Regulation

- Definitions under GDPR
    - Data Controller
    - Data Processor
    - Data Subject
    - Personal Data
    - Special Personal Data
    - Fairness and lawfulness
    - Purpose limitation
    - Proportionality
    - Accuracy, Storage limitation, Integrity, and confidentiality
    - Privacy by Design and Accountability (Responsibility of controllers and processors
    - Data protection by design and by default

- Who is protected by GDPR?
- When does Data Protection Law Apply?
- Which activities are covered?
- Processing Personal Information
- Exclusions – Article 84 GDPR
- Principles of Data Protection
- Rights of Data Subjects
- The Data Protection Commission
- Offences/breaches under GDPR
- Data Transfer to Third Countries – Article 44-50
- Capturing consent as part of the GDPR
- The Right to be forgotten

2.11.7 Module teaching and learning (including formative assessment) strategy

The module uses participative lectures, which consist of tutorial-style discussions, group work sessions and exercises. The lectures are supplemented by structured on-line resources and directed reading. Formative assessment is provided in the form of interactive exercises such as directed class discussion topics which reference current affairs pertaining to Privacy and Data Protection Law at the time of instruction. Formative assessment is also provided though tutorial-style discussions, group work and exercises. These focus on specific case law and problem-based learning requiring learners to analyse the law and apply it to both privacy and data protection disputes or issues.

Learners also engage in collaborative work in pairs or small groups to brainstorm what learning has been achieved at the end of lectures. In order to support learners through the examination process, they engage in the answering of sample examination questions and correction of their own or peer's papers, thereby familiarising themselves with the marking criteria. Learners also engage in activities where they draft their own exam questions in order to recap and consolidate a particular topic.

Learners undertaking the course via blended learning benefit from varied and additional options for engagement to compensate their reduced attendance of campus. These include

webinars, screencasts (recorded lectures), discussion fora, and increased use of the College's VLE (Virtual Learning Environment), Moodle.

In addition to what has been stated, classroom assessment and benchmarking techniques are deployed to encourage learners to develop more agency in terms of their own learning including in-class presentations, group work, peer-review exercises and reflective practice. The variety of teaching, learning and assessment techniques reflect an enhanced emphasis on skills acquisition to deepen practical knowledge. Finally, the attention of learners is drawn to current industry practice and technology used in the specific area of law to add a further dimension to learning, tracking the actual practice of legal professionals.

2.11.8 Work-based learning and practice-placement

Privacy and Data Protection Law is a 5 ECTS credit module and does not require work-based learning and practice placement.

2.11.9 E-learning

Moodle, the College Virtual Learning Environment, is used to disseminate notes, advice, and online resources to support the learners. Moodle can be accessed in the learner's home, various open labs on campus and in the library. The learners are also given access to Lynda.com as a resource for reference.

2.11.10 Module physical resource requirements

Requirements are for a fully equipped classroom. The classroom is equipped with a PC and Microsoft Office; no other software is required for this module.

The College library has a dedicated law section and online legal research tools (JustisOne, Westlaw, Hein Online).

2.11.11 Reading lists and other information resources

Primary Reading

Kelleher, D. and Murray, K. (2018) EU Data Protection Law, London: Bloomsbury Publishing
Massey, S. (2017) The Ultimate GDPR Practitioner Guide: Demystifying Privacy & Data Protection, Fox Red Risk, United Kingdom (2017)
Leenes, R. van Brakel, R. Gutwirth, S. De Hert, P. (2017) Data Protection and Privacy: The Internet of Bodies, Oxford: Bloomsbury Publishing
Kelleher, D. (2015) Privacy and Data Protection Law in Ireland, Dublin: Bloomsbury Professional
Murray, A. (2016) Information Technology Law, Oxford: Oxford University Press

Secondary Reading

Millard, C. (2013) Cloud Computing Law. Oxford: Oxford University Press.
Voigt, P. von dem Bussche, A. The EU General Data Protection Regulation (GDPR)- A Practical Guide, London: Springer Publishing
Foulsham, M. & Hitchen, B. (2017) GDPR: Guiding Your Business To Compliance: A practical guide to meeting GDPR regulations. London: Amazon

Alsmadi, I., Burdwell, R., Aleroud, A., Wahbeh, A., Qudah, M., Al-Omari, A. (2018). Practical Information Security. United States: Springer Publishing.

2.11.12 Specifications for module staffing requirements

Lecturers are expected to hold at least a level 8 legal qualification, preferably with a professional legal qualification and specific practical expertise in the area of data protection and e-Privacy. It is an advantage to have completed the Certificate in Training and Education provided by Griffith College.

Preference will be given to Lecturers who can demonstrate practical qualifications in Privacy from reputable organisations such as the IAPP.
Learners also benefit from the support of the Programme Director, Programme Administrator, Lecturers, Learner Representative, Students Union and Counselling Service.

2.11.13 Module summative assessment strategy

Theoretical knowledge is assessed by an end of module examination worth 100% of the total marks in this subject.

The assessed work breakdown can be seen in the table below.

No	Description	MIMLOs	Weighting
1	Exam	i, ii, iii, iv, v, vi, vii	100%

2.11.14 Sample assessment materials

Sample Examination
Learners are required to answer Question 1 (Compulsory Multiple Choice Questions). In addition to Question 1 learners are required to answer one question from Questions 2 and 3 (Privacy) and one question from Questions 4 and 5 (Data Protection).

Compulsory Question - Question 1
Multiple Choice Questions – Data Protection

Question 1
Which European Union (EU) legal document forms the basis for all EU privacy and data protection legislation?
A. UN Universal Declaration of Human Rights
B. DIRECTIVE 95/46/EC
C. EU Charter of Fundamental Rights
D. General Data Protection Regulation

Question 2
The GDPR does not describe the concept of 'privacy'. Which European Union (EU) legal document contains an Article 7 on 'respect for private and family life'?
A. EU Charter of Fundamental Rights

B. DIRECTIVE 95/46/EC
C. General Data Protection Regulation
D. DIRECTIVE 2016/680

Question 3
Which legal document forms the cornerstone for all privacy legislation?
A. European Convention on Human Rights
B. EU Charter of Fundamental Rights
C. Universal Declaration of Human Rights
D. EC Implementing Decision 2016-7-12 (EU-US Privacy Shield)

Question 4

Which type of EU legislation does apply directly to all member states?
A. Directive
B. Decision
C. Executive order
D. Regulation

Question 5
The GDPR defines a certain role as "... the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." Which role is this?
A. Processor
B. Controller
C. Supervisory authority
D. Data protection officer

Question 6
Who is responsible for the internal data protection organisation of the EU?
A. European Data Protection Board
B. European Data Protection Supervisor
C. Independent supervisory authority
D. Article 29 Working Party

Question 7
Which sections of the GDPR set out the reasons for the contents of the enacting terms and help you better understand the GDPR?
A. Citations
B. Articles
C. General provisions
D. Recitals

Question 8
Which of the following activities belong to the material scope of the GDPR?
A. Member States carrying out activities for the Common Foreign and Security Policy

B. Processing of personal data wholly or partly by automated means
C. Natural persons in the course of a purely personal or household activity
D. Processing by competent authorities for the purposes of the prevention of criminal offences

Question 9
Chapter I of the GDPR outlines the general provisions for the act. Which of the articles describes that the GDPR does not apply to natural persons in the course of a purely personal or household activity?
A. Article 2 Material scope
B. Article 3 Territorial scope
C. Article 4 Definitions
D. Article 1 Subject-matter and objectives

Question 10
What is the territorial scope of the GDPR?
A. EU
B. EEA
C. EFTA
D. UN

Question 11
Which of the following is NOT considered 'personal data' by the GDPR?
A. Sensitive personal data
B. Pseudonymised personal data
C. Anonymised personal data
D. Biometric data

Question 12
The GDPR states "... whether or not they are performed by automated means." What official definition is this part of?
A. Controlling
B. Purpose limitation
C. Processing
D. Storage limitation

Question 13
Which of the following activities falls outside the scope of the GDPR?
A. Profiling
B. Anonymisation
C. Storing
D. Erasing

Question 14
Which of the GDPR principles for processing is not absolute and will depend on the specific goal(s) for which the data is processed?

A. Accuracy
B. Purpose limitation
C. Storage limitation
D. Integrity and confidentiality

Question 15
Which GDPR principle for processing states that personal data may only be collected for explicit purposes?
A. Purpose limitation
B. Lawfulness, fairness and transparency
C. Data minimisation
D. Storage limitation

Question 16
Under certain circumstances, who can obtain restriction of processing?
A. Controller
B. Processor
C. Representative
D. Data subject

Question 17
What may cause an exception to the restriction on the processing of sensitive personal data?
A. The data must be processed for marketing purposes
B. The data subject himself has made the data public.
C. The data is archived by the controller.

Question 18
For some categories of personal data, EU member states may maintain or introduce further conditions on the processing of sensitive data. For what type of sensitive data may this be the case?
A. Data concerning health
B. Data processed to make legal claims
C. Data of substantial public interest
D. Data stored for legitimate archiving purposes

Question 19
Apart from the rules laid down in the GDPR, member states also have room to provide exemptions for the certain types of processing. What is an example of such an additional type of processing?
A. Processing of sensitive data
B. Processing of anonymised personal data
C. Processing by churches and religious associations

Question 20
What right does the data subject have to correct inaccurate personal data?

A. Rectification
B. Data portability
C. Not to be profiled
D. Withdraw consent

Question 21
A controller informs a data subject that her personal data is no longer necessary and will be destroyed. How can the data subject prevent erasure and impose restriction of processing instead?
A. Claim that the data is required exercise of legal claims
B. Withdraw consent for the processing
C. Exercise her right to rectification

Question 22
According to the GDPR, which is NOT a legitimate reason for the transfer of personal data to 'third countries'?
A. The transfer is covered by binding corporate rules
B. It is demanded by a US presidential order
C. There is an EC adequacy decision
D. The controller had provided appropriate safeguards

Question 23
The GDPR stipulates that ...appropriate and effective measures shall be taken to demonstrate the compliance of processing activities. Who is responsible and accountable?
A. The processor
B. The independent authority
C. The data subject
D. The controller

Question 24
Which is NOT one of the 7 foundational principles?
A. Integrity and confidentiality
B. Visibility and transparency
C. Privacy embedded
D. Full functionality, positive sum

Question 25
A software company takes data protection into account when developing applications. Of what is this an example?
A. Data protection by default
B. Legitimate data protection
C. Data protection by design
D. Organisational data protection

Question 26

Both the controller and the processor are obliged to keep records of processing activities. What is one of the records that needs to be kept (at least) by the processor?
A. Name and contact details of the DPO
B. Data retention information
C. Security measures

Question 27
The GDPR states that "The controller and the processor and, where applicable, their representatives, shall cooperate ... with the supervisory authority in the performance of its tasks." When is this required?
A. Pro-actively
B. On request
C. When required by national law
D. During processing

Question 28
According to the GDPR, a Data Protection Impact Assessment (DPIA) is required in certain particular circumstances. What is NOT such a particular circumstance?
A. Systematic monitoring of public areas on a large scale.
B. Systematic extensive evaluating of personal aspects.
C. Whenever using new technologies.
D. When processing data for exercise or defence of legal claims

Question 29
With whom does the GDPR prescribe transparent communications regarding processing?
A. The data subject, recipients and the DPA
B. The data subject, the processor and the DPA
C. The processor, the recipients and the DPO

Question 30
The GDPR requires a transparent way of communicating with a data subject. What does this mean?
A. Concise
B. Intelligible
C. In clear and plain language
D. All of the above

Question 31
In what case does the controller need to inform the data subject concerning a breach of his/her personal data?
A. When the data breach results in the loss of encrypted personal data
B. After rectification or erasure of personal data, or after restriction of processing
C. When the data breach is likely to result in a high risk to the rights and freedoms of the data subject

Question 32
A processor has erased personal data. In what case does the controller NOT have to inform each and every recipient of the personal data?
A. If the personal data was processed with conscious consent by the data subject
B. If the personal data was outdated anyway
C. If this proves impossible or involves disproportionate effort
D. If the data was erased in an irreversible way

Question 33
In some cases, the DPA needs to be consulted prior to processing. What is an example of such a case?
A. A new subsidiary is added to the binding corporate rules
B. A data subject claims his/her right of access to the personal data
C. A data breach occurred compromising the data subject's personal data
D. A DPIA indicates that processing will involve a high risk that cannot be mitigated

Question 34
When does the data breach notification obligation apply?
A. When a security breach involves personal data
B. When a data breach has occurred
C. When a risk analysis indicates that there are vulnerabilities in the processing system
D. When a data subject retracts his/her consent for the processing of personal data

Question 35
When does the data breach notification obligation apply?
A. When a data breach leads to a considerable likelihood of serious adverse effects on the protection of personal data
B. When the data breach has serious adverse effects on the protection of personal data
C. When the personal data breach is likely to result in a risk to the rights and freedoms of natural persons
D. All of the above

Question 36
What does the term 'accountability' refer to in the GDPR?
A. The obligation to be able to demonstrate compliance with the GDPR
B. The legal certainty that accountability does not apply when compliance with the GDPR can be demonstrated
C. The application of mechanisms that can reduce the risks to the processing of personal data

Question 37
According to the GDPR, in what way can compliance with the GDPR be demonstrated?
A. Adherence to a code of conduct
B. Keeping records
C. Setting up written and binding data protection policies
D. All of the above

Question 38
What entity is authorised to monitor compliance with an approved code of conduct?
A. An accredited certification body
B. The independent supervisory authority
C. The European Data Protection Board
D. The data protection officer

Question 39
What investigative and corrective power does the independent supervisory authority have?
A. The DPA can order a temporary limitation on processing
B. The DPA can order a definitive limitation on processing
C. The DPA can order the suspension of data flows
D. All of these

Question 40
What is the maximum penalty the DPA can hand out for infringements of the processing principles?
A. Up to €10m or 2% of the total worldwide annual turnover
B. Up to €20m or 4% of the total worldwide annual turnover
C. Criminal fines and prison sentences

Answers Question	Answer	Question	Answer
1	C	21	A
2	A	22	B
3	C	23	D
4	D	24	A
5	B	25	C
6	B	26	A
7	D	27	B
8	B	28	D
9	A	29	A
10	B	30	D
11	C	31	C
12	C	32	C
13	B	33	D
14	A	34	B
15	A	35	D
16	D	36	A
17	B	37	D
18	A	38	A
19	C	39	D
20	A	40	B

Learners must answer one of Question 2 or Question 3 (Privacy)

Question 2
John previously completed a degree in psycho-analysis at Walsam College and applied to sit the entrance examination to become a psycho-analyst. Candidates can take up to six attempts to pass the exams over the course of three years, with two sittings per year. John has now reached his final sitting, having failed the previous five sittings. In order to assist in his preparations John has asked Walsam College to provide him with copies of his five exam scripts, however, they have declined.

Advise John on his right to access past exam scripts referring to relevant case law.

Sample Answer 2

In 2016 the Irish Supreme Court handed down a decision in the long-running case of Nowak v. Data Protection Commissioner [2016] IESC 18. The Supreme Court's decision, its first ever data protection ruling, means that the Court of Justice of the European Union ("CJEU") must now decide whether an exam candidate's script constitutes personal data.

Mr. Nowak's long-running legal battle has been heard by four separate rungs of the Irish courts system.

Mr. Nowak failed, on three separate occasions, one of the mandatory exams to become a chartered accountant. Mr. Nowak then submitted a request under Section 4 of the Irish Data Protection Acts 1988 and 2003 ("DPA") seeking all personal data held by the relevant examining body. That body declined to release his examination script on the basis that it did not constitute personal data within the meaning of the DPA.

Mr. Nowak contended that his examination script constitutes his personal data because:
it contains his handwriting, which he contends is biometric data; and
it may contain markings and/or comments by the examiner.

Mr. Nowak submitted a formal complaint to the Irish Data Protection Commissioner. He disputed the assertion that his examination script does not constitute personal data. The DPC refused to investigate the complaint under Section 10(1)(b)(i) of the DPA. The DPC was of the opinion that Mr. Nowak's complaint was "frivolous and vexatious".

Mr. Nowak appealed this decision to Ireland's Circuit Court. When the Circuit Court upheld the DPC's decision, further appeals were made to the High Court and, subsequently, the newly established Court of Appeal. The matter eventually found its way to the Supreme Court.

A number of matters were examined by the Irish Supreme Court. These included whether Mr. Nowak enjoyed a right of appeal in the Irish Courts under the DPA and what form these appeals may take.
Of most interest to privacy and data protection professionals will be the Supreme Court's examination of Mr. Nowak's assertion that his examination script is his personal data. Mr. Justice O'Donnell, writing the unanimous decision for the Court stated:
The underlying issue here, whether an examination script is ever capable of being personal data within the meaning of the [DPA], and if so, whether this script is such personal data, is one of some difficulty and complexity that requires the analysis of a number of different texts and provisions.

The Supreme Court went on to review how the term 'personal data' is defined in both the DPA and the Data Protection Directive (95/46/EC).
The DPC relied on previous analysis by Advocate General Sharpston in the YS case where she stated that:
… only information relating to facts about an individual can be personal data. Except for the fact that it exists, a legal analysis is not such a fact. Thus, for example, a person's address is personal data but an analysis of his domicile for legal purposes is not.

Mr. Nowak cited Section 4(6)(b) of the DPA which prevents the DPA being used by exam candidates to circumvent the publication of exam results. Mr. Nowak argued that Section 4(6)(b) implicitly recognises that examination results constitute personal data. If examination results constitute personal data, Mr. Nowak argued that the raw material from which results are derived must also be personal data. Such raw material would include an examination script and examiner's comments or marks.

The Supreme Court decided that this "is ultimately a matter of European law". The Court wasn't satisfied that the issue at hand was reasonably clear and free from doubt. In such circumstances, it decided to refer the question as to whether an examination script is capable of constituting personal data to the CJEU.

Subsequently the European Court of Justice (ECJ) ruled that a written exam paper amounts to personal data and can be accessed by its author.

An opinion document issued by the ECJ Advocate General (opinion documents precede ECJ rulings but do not always reflect eventual outcomes) found the content of exam papers did in fact make for personal data.

The Advocate General told the ECJ the Irish Data Protection Commissioner was wrong to tell Mr Nowak he had no right of access to his failed paper.

On Wednesday, the ECJ upheld that view, stating rights of access to data provided for in European law "may also be asserted in relation to the written answers submitted by a candidate at a professional examination and to any comments made by an examiner with respect to those answers".

"The court holds that to give a candidate a right of access to those answers and to those comments serves the purpose of the directive of guaranteeing the protection of that candidate's right to privacy with regard to the processing of data relating to him, irrespective of whether that candidate does or does not also have such a right of access under the national legislation."

Question 3
The right to privacy in Ireland is guaranteed.

Discuss the above statement with reference to the Constitution, relevant case law, ECHR, relevant legislation (domestic and European).

Sample Answer 3
The right to privacy in Ireland is guaranteed both in our constitution and on a European level.
Article 40.3 of the 1937 Constitution of Ireland states that:

> *"The State guarantees in its laws to respect, and as far as practicable, by its laws to defend and vindicate the personal rights of the citizen."*

> *"The right to privacy was first recognised in this jurisdiction in McGee v Attorney General, Walsh J. in the Supreme Court held that "Article 41 of the Constitution guarantees the husband and wife against……invasion of their privacy by the State."*

In Kennedy and Arnold v Attorney General, Hamilton P held that the right to privacy was one of the unenumerated rights recognised by Article 40.3 of the Constitution.

Article 8 of the European Convention on Human Rights (hereafter referred to as the 'ECHR') is entitled "Right to respect for personal and family life" and it states that:

> *'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 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.'*

Rights under the ECHR are used as a justification for the enactment of Directive 95/46. At recital 2, the Directive sets out that the design of data processing systems "must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy"

The ECHR became part of Ireland's domestic law on the commencement of the European Convention on Human Rights Act 2003. Section 2(1) of the Act provides :

> *'in interpreting and applying any statutory provision or rule of law, a court shall, in so far as is possible, subject to the rules of law relating to such*

interpretation and application, do so in a manner compatible with the State's obligations under the Convention provisions.

Privacy clearly exists as a right in both the Constitution and the ECHR.

This European Convention on Human Rights Act 2003 requires that the Data Protection Acts must be interpreted in a manner compatible with the ECHR.

The Oireachtas has yet to regulate for a general right to privacy, however, the Data Protection Acts, EU Directives and General Data Protection Regulation are a variety of legislation which does create more specific privacy rights.

Despite the existence of all the above safeguards, in the pragmatic sense there is little protection afforded to us in the context of privacy rights.

In addition to these existing safeguards to the right to privacy there is also a proposed new Privacy Bill 2012. The purpose of the Bill is to provide for a new tort of violation of privacy taking into account the jurisprudence of our courts and the European Court of Human Rights.
Section 2 provides that it is a tort for a person wilfully and without lawful authority to violate the privacy of an individual. The tort is actionable without proof of special damages.

Section 5 provides for a number of defences to an allegation of violation of privacy. These essentially involve where the act was that of a public servant acting or reasonably believing themselves to be acting in the course of their duties, etc.

Section 7 provides a jurisdiction for actions taken in the Circuit Court where the claim does not exceed €50,000.

Learners must answer one of Question 4 or Question 5 (Data Protection)

Question 4
Simon has recently commenced employment with NoWay Ltd. a subsidiary of Big Holiday Ltd., a group of travel agencies which specialise in adventure holidays for the over 65's. When speaking to colleagues it became apparent NoWay Ltd. retains personal information on all clients including previous clients (name, address, date of birth, health conditions, BIC/IBAN, email address, next of kin, ethnicity and religious belief). Simon notices that mass emails are occasionally sent to previous clients with new offers, without using the Blind Carbon Copy (BCC) option. Simon asks to speak to the Data Protection Officer (DPO), however, he is informed that they do not have a DPO. Simon is not an expert on GDPR but remembers that his previous employer had a DPO. Simon approaches you for the following advice;

- Does every company need a Data Protection Officer?
- When must a Data Protection Officer be designated?

- Can a company appoint an external DPO instead of an internal DPO?
- Who is a Data Controller and Data Processor and can you give an example of their relationship?

Sample Answer

The GDPR calls for the mandatory appointment of a Data Protection Officer for any organization that processes or stores large amounts of personal data, whether for employees, individuals outside the organisation, or both. DPOs must be "appointed for all public authorities, and where the core activities of the controller or the processor involve 'regular and systematic monitoring of data subjects on a large scale' or where the entity conducts large-scale processing of 'special categories of personal data,'" like that which details race or ethnicity or religious beliefs.

The data protection officer is a mandatory role under Article 37 for all companies that collect or process EU citizens' personal data. DPOs are responsible for educating the company and its employees on important compliance requirements, training staff involved in data processing, and conducting regular security audits. DPOs also serve as the point of contact between the company and any Supervisory Authorities (SAs) that oversee activities related to data.

The data controller and the data processor must designate a data protection officer in any case if:
a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 GDPR and personal data relating to criminal convictions and offences referred to in Article 10 GDPR. (Art. 37 Para. 1 GDPR)

National legislations have the right to define further circumstances in which a data protection officer must be designated below the abovementioned thresholds (e.g. BDSG-neu in Germany).

Not every enterprise is required to designate a separate data protection officer. For example, a group of companies may designate a joint data protection officer. Associations and organizations of which the controller or processor is a member may also designate a data protection officer.

NoWay Ltd. may be required to appoint a data controller or data processor. A Data Controller has the most responsibility when it comes to protecting the privacy and rights of the data's subject, such as the user of a website. Simply put, the data controller controls the procedures and purpose of data usage and will

be the one to dictate how and why data is going to be used by the organisation. A data controller can process collected data using its own processes. In some instances, however, a data controller needs to work with a third-party or an external service in order to work with the data that has been gathered. Even in this situation, the data controller will not relinquish control of the data to the third-party service. The data controller will remain in control by specifying how the data is going to be used and processed by that external service.
A data processor simply processes any data that the data controller gives them. For example, the data processor may be a third-party company that the data controller chose to use and process the data. The data processor does not own the data that they process nor do they control it. This means that the data processor will not be able to change the purpose and the means in which the data is used. Furthermore, data processors are bound by the instructions given by the data controller.

For instance, NoWay Ltd. has a website that collects data on the pages their visitors visit. This includes the page they enter the site with, the pages that they visited next, and how long they stayed in each page. NoWay Ltd. is the data controller, as they decide how all of this information is going to be used and processed, and for what purpose. NoWay Ltd. uses AnalyseThisAnalytics to find out which of their pages are most popular and which ones are making website visitors leave. This helps them plan their content better by knowing exactly how much time each visitor spends on a particular page. Not only does NoWay Ltd. know which topics to write on, but also discover new topics that might be of interest to their customers. Plus, it helps them improve on the content that is already there. NoWay Ltd. needs to share the data that they get to AnalyseThisAnalytics in order to get the insights they want from AnalyseThisAnalytics. In this case, AnalyseThisAnalytics is the data processor.

Learners should also refer to the qualifications, further responsibilities and requirements in respect the DPO, data controller and data processor.

Question 5
What are the new principles created by GDPR, the key differences between GDPR and Directive 95/46/EC and the essential new regulations on data security under GDPR?

Sample Answer 5
GDPR does not abrogate current principles of personal data processing. In particular, the GDPR maintains the four elementary principles of Directive 95/46/EC:

Prohibition unless consent is obtained or processing is based on another legal ground (""Processing shall be lawful only if and to the extent that at least one of the following applies ..."") (Art. 6 Para. 1 GDPR). This states a general prohibition unless authorised.

Purpose limitation (Art. 6 Para. 4, Art. 5 Para. 1 Subpara. b GDPR);

Transparency (Art. 13 & 14 GDPR);

Rights of data subjects (Art. 15 ff. GDPR).

Compared to Directive 95/46/EC, GDPR does stipulate more obligations for data controllers and data processors in regard to their documentation of fulfilment of the GDPR requirements by organisational measures, as well as changes in the territorial scope of EU privacy regulation.

In particular:

- *territorial scope (Art. 3 GDPR)*
- *accountability (Art. 5 Para. 2 GDPR)*
- *obligations for controllers relating to the rights of data subjects (Art. 12 GDPR)*
- *obligation for organisation of the controller (Art. 24 GDPR)*
- *data protection by design and by default (Art. 25 GDPR) (combined with ""data minimisation"" (Art. 5 Para. 1 Subpara c GDPR))*
- *data breach notification (Artt. 33 & 34 GDPR)*
- *data protection impact assessment (Art. 35 GDPR), consultation of controlling authorities (Art. 36 GDPR)*
- *the data protection officer (Artt. 37 ff. GDPR)*
- *administrative sanctions (Art. 83 GDPR)*
- *joint liability of controller and processor under the requirements of Art. 82 GDPR.*

This means that the fundamental new aspect is the principle of comprehensive obligations for documentation and organisation of the observance of data security at the controller (enterprise).

GDPR emphasises the obligation to safeguard personal data. Under the GDPR, data security is still a substantial element of privacy and data protection. In comparison to Directive 95/46/EC, the regulations on data security are redesigned in GDPR so that more and new aspects must be considered for defining adequate measures for data security.

Under GDPR, the performance of appropriate documentation becomes an element of the evaluation whether data may be processed. In the course of a data protection impact assessment in particular, the provision of adequate data protection must be evaluated and documented (Art. 35 GDPR).

The main differences concerning the obtainment of consent compared to Directive 95/46/EC are threefold:

Transparency for the data subject is emphasized more heavily (cf. Art. 4 No. 11 GDPR)

The data subject must be informed about his or her right to withdraw consent (cf. Art. 7 Para. 3 GDPR)

Special conditions apply to consent given by children relating to online services (cf. Art. 8 GDPR). Furthermore, there is doubt whether implied consent is sufficient under the GDPR. If there are multiple purposes for the processing, consent should be obtained for all of them