OFFSHORE TRAINING

GDPR – Are You in the Know?

Tutor – Vicky Le Poidevin

27th February 2019

GDPR and The Data Protection (Bailiwick of Guernsey) Law, 2017

Effective date
GDPR came into effect for EU Member States on 25 May 2018.

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Law") came into effect on the 25 May 2018; there were number of transitional arrangements, which ends in May 2019.

Who does GDPR affect?

The GDPR applies to organisations within the EU and organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects.

It applies to all entities processing and holding the personal data of data subjects residing in the European Union, regardless of the entity's (or in your case, charities') location.

Who does the Law affect?

Like GDPR, the Law applies to organisations located in Guernsey, and Entities and Charities offering services to Guernsey Data Subjects.

Fines and penalties

What are the maximum penalties for non-compliance with GDPR?

Under GDPR, organisations can be fined up to 4% of annual global turnover or €20 Million for breaching GDPR.

What are the maximum penalties for non-compliance with the Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Law")?

Under the Law, administrative fine issued against a person are capped at:

- either £10,000,000, or
- any higher or lower limit prescribed by Ordinance made by the States of Deliberation in place of the limit in paragraph (a).

An administrative fine issued will not exceed £300,000 unless the amount of the fine is less than 10% of the total global annual turnover or total global gross income in the preceding financial year of that person.

An administrative fine issued against a person must not exceed 10% of the total global annual turnover or total global gross income of that person during the period of the breach in question, up to a maximum period of 3 years.

What is the purpose of GDPR and the Law?

- ❑ Standardise Data Protection Law across the EU
- ❑ Make it easier for people to understand what companies (and charities) are doing with their personal data
- ❑ The Law puts us on a level playing field to parties complying with GDPR but under our own Guernsey specific law

What is personal data?

What does The Law say?

A **"personal data"** means any information relating to an identified or identifiable individual

B **1. Identifiable individual.**

An individual is identifiable from any information where the individual can be directly or indirectly identified from the information, including –

(a) by reference to a name or an identifier,
(b) by reference to one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity,
(c) where, despite pseudonymisation, that information is capable of being attributed to that individual by the use of additional information, or
(d) by any other means reasonably likely to be used, taking into account objective factors such as technological factors and the cost and amount of time required for identification in the light of the available technology at the time of processing.

"data subject", in relation to personal data, means the identified or identifiable individual to whom the personal data relates

What is personal data?

What does this mean for your charity?

This can include:

- Name
- Photo
- Email address
- Bank details
- Medical / Disability information
- Computer IP address
- Payroll data
- Sickness records
- Expenses claims
- Employment Records
- And much more…

Key Data Protection Principals

What are the key principals of GDPR and the Law?

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

What is a Privacy Notice and what is it trying to achieve?

What does The Law say?

C **Right to information for personal data collected from data subject.**

12. (2)"……the data subject has a right to be given the following information in accordance with subsection (3) –
(a) the information specified in Schedule 3, and
(b) a statement as to
(i) whether the provision of the personal data by the data subject is a statutory or contractual requirement, or a requirement necessary to be met in order to enter into a contract, and
(ii) whether the data subject is obliged to provide the personal data, and the possible consequences of failure to provide that personal data.

(3) The controller must give the data subject that information before or at the time the personal data is collected from the data subject.

What is a Privacy Notice and what is it trying to achieve?

What does the Law say? (cont'd)

D 13.

(1) Where personal data processed in the context of a controller has not been collected from the data subject by either the controller or a processor acting on the controller's behalf, the data subject has a right to be given the information specified in Schedule 3 in accordance with subsection (2).

(2) The controller must give the data subject that information –
(a) within a reasonable period of that personal data being so processed, having regard to the specific circumstances in which the personal data is so processed, and
(b) in any case, before or at the earliest occurrence of any of the following times –
(i) if the personal data is used for communication with the data subject, the time of the first communication with the data subject,
(ii) if the personal data is disclosed to another recipient, the time when the personal data is first disclosed to any recipient, and
(iii) the expiry of one month following the processing of the personal data.

What is a Privacy Notice and what is it trying to achieve? – cont'd

- What does this mean for your charity?
- How can you draft this?

What is a personal data breach?

What does The Law say?

E **"personal data breach"** means a breach of security leading to –

(a) accidental or unlawful destruction, loss, or alteration of, or
(b) unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed,

Examples of possible data breaches:

- Access to data by an unauthorised third party
- Changing personal data without permission of the Data subject
- Deliberate or accidental action (or inaction) by a controller or processor
- Computer / Phones / Other technology devices containing personal data being lost or stolen
- Not being able to access personal data
- Personal or sensitive data being sent to an incorrect recipient
- When any personal data is lost, destroyed, corrupted or disclosed
- If an unauthorised person sees or passes on data without proper authorisation

What to do if there is a data breach:

What does The Law say?

F **42.** (2) Where a controller becomes aware of a personal data breach, the controller must give the Authority written notice of it as soon as practicable, and in any event, no later than 72 hours after becoming so aware, unless this is not practicable

42. (5) Subsection (2) does not apply where the personal data breach is unlikely to result in any risk to the significant interests of the data subject.

42. (6) In any case, a controller must keep a written record of each personal data breach of which the controller is aware –
(a) the facts relating to the breach,
(b) the effects of the breach,
(c) the remedial action taken, and
(d) any steps taken by the controller to comply with this section, including whether the controller gave a notice to the Authority under subsection (2), and if so, a copy of the notice.

43. (1) Where a controller becomes aware of a personal data breach that is likely to pose a high risk to the significant interests of a data subject, the controller must give the data subject written notice of the breach as soon as practicable (see exclusions and more data in the law)

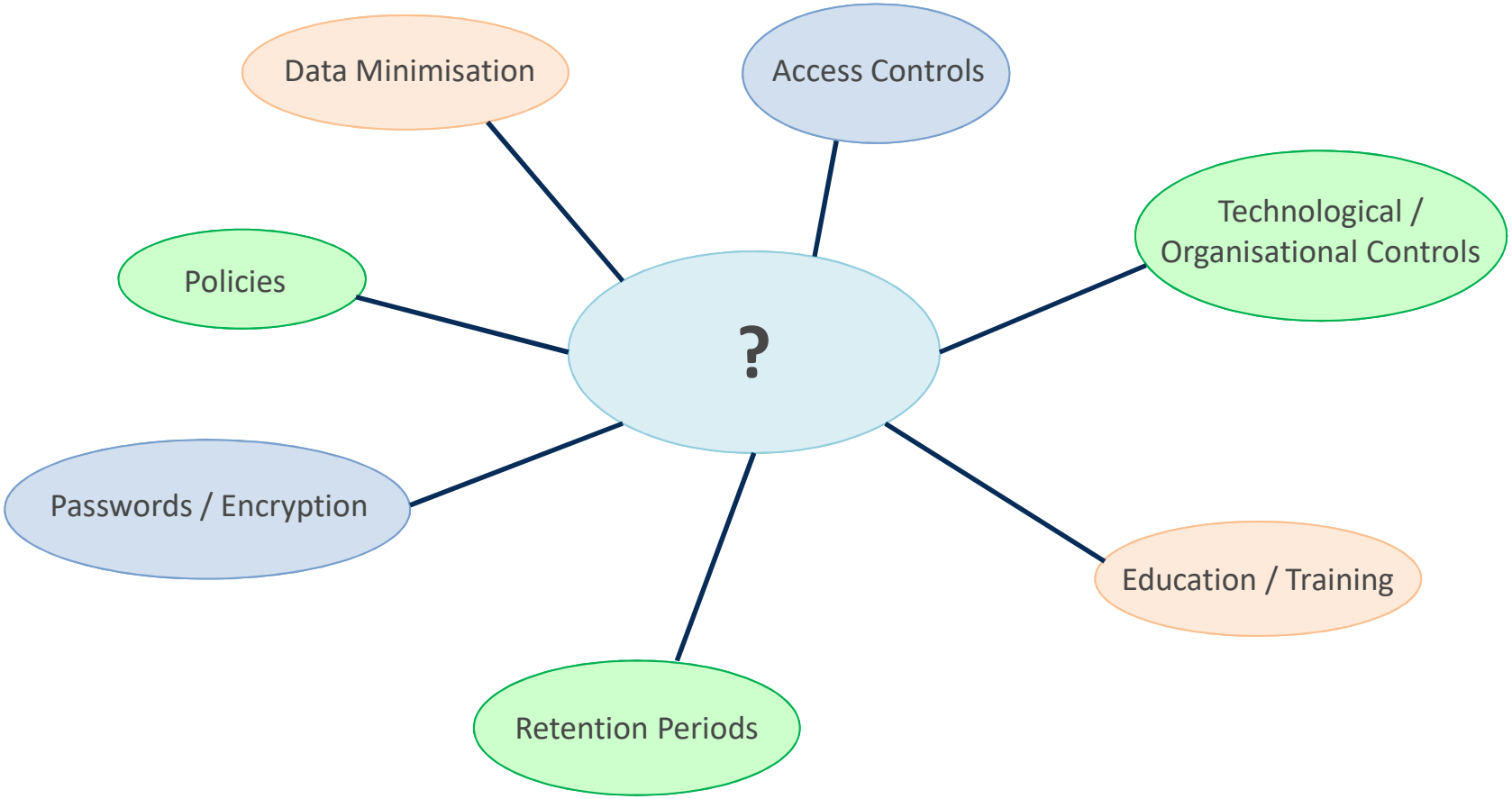
What to do if there is a data breach – cont'd

What does this mean for your charity?

- ❑ How will you identify a breach?
- ❑ Do all parties know who to report data breaches to in your charity?
- ❑ How do I tell the authority?
- ❑ Do you have a procedure in place?
- ❑ Can you respond in 72 hours?

OFFSHORE TRAINING

How to try and avoid a data breach:



Subject Access Request

What does The Law say?

G

14. Right to data portability.

15. Right of access.

16. Exception to right of portability or access involving disclosure of another individual's personal data.

17. Right to object to processing for direct marketing purposes.

18. Right to object to processing on grounds of public interest.

19. Right to object to processing for historical or scientific purposes.

20. Right to rectification.

21. Right to erasure.

22. Right to restriction of processing.

23. Right to be notified of rectification, erasure and restrictions.

24. Right not to be subject to decisions based on automated processing.

25. Controller must facilitate exercise of data subject rights.

Subject Access Request – cont'd

What is a "SAR"?

A request by a data subject (an individual) to see

- What personal data your charity holds about them
- Why your charity is holding it
- Who their information is disclosed to by your charity
- Other Data as outlined in Schedule 3

This could be a client, employee, ex-employee or any other natural person (aka individual) that your charity holds personal data on /about.

You usually have 30 days to respond so it is really important requests are dealt with promptly.

Do parties have to quote “SAR”?

A data subject does not have to use the phrase 'subject access request' or quote GDPR the Law. They just have to be clear that they are asking for their own personal data.

Does the request have to be in writing?

A data subject does not need to make the request in writing, it can be verbal.

If a data subject makes a request electronically, your charity should provide the information in a commonly used electronic format, unless the individual requests otherwise.

What is the best way to provide data to the data subject?

Where the data subject makes the request by electronic form means, the information should be provided by electronic means (machine readable) where possible, unless otherwise requested by the data subject.

A best practice recommendation is that, where possible, organisations should provide remote access to a remote data base providing the Data Subject with direct access to his or her information – but this can not include other parties data or you would be potentially breaching GDPR the Law!

Practical Case Study

We will now work through a practical case study to help you apply the Law to your organisation.

This case study focuses on:

- Types of personal data held by charities
- Who has access to the personal data
- Access controls and security over the personal data
- If the data is transferred for processing outside the EU
- Retention periods
- If the data is special category and its implications

Who are we?

About the team

Vicky Le Poidevin - Senior Manager Consulting and Training

Vicky has 18 years' experience in the finance sector. Vicky's strengths include projects focused on reducing costs, risks and resource requirements of businesses through the creation and redesign of controls and processes. Vicky has completed the EU GDPR Foundation qualification and has used the knowledge to assist with a number of GDPR cases over the last 9 months.

Will Morgan - Managing Director of Offshore

In 2001 Will joined EY in an audit role and qualified with the Institute of Chartered Accountants of Scotland. Will provides training and operational solutions to businesses to help them improve the efficiency and effectiveness of their team.
As a business owner, Will is cognisant of the day to day challenges GDPR can bring to small businesses.

About Offshore

Company

Offshore was formed in 2007 by Will Morgan who remains the majority company shareholder. Offshore provide both accounting and consulting services to a wide range of businesses in Guernsey, Jersey and Dublin. Annual fee turnover is approximately £3m.

Staff

The company now employs 36 professionals within the business to service its client base from its office on Les Bas Courtils Road in Guernsey. Offshore believe that the businesses strength is that all staff have come from industry and therefore have a sound understanding of client operations and expectations.

Our Clients

The majority of the assignments that we undertake result in a monthly delivery to our clients in order to meet both management and/or regulatory requirements. We are used to interacting with external parties and auditors and are familiar with them being on site to complete the field work and ask questions.

Please note that this document and the presentation provided is intended to provide training materials in respect to a one off training session provided by Offshore Consulting (Guernsey) Limited to members of the Association of Guernsey charities.

The training was not designed to provide specific financial or legal advice and should not be relied upon as such by any party.

Offshore Consulting (Guernsey) Limited accepts no liability arising from the use of these materials.