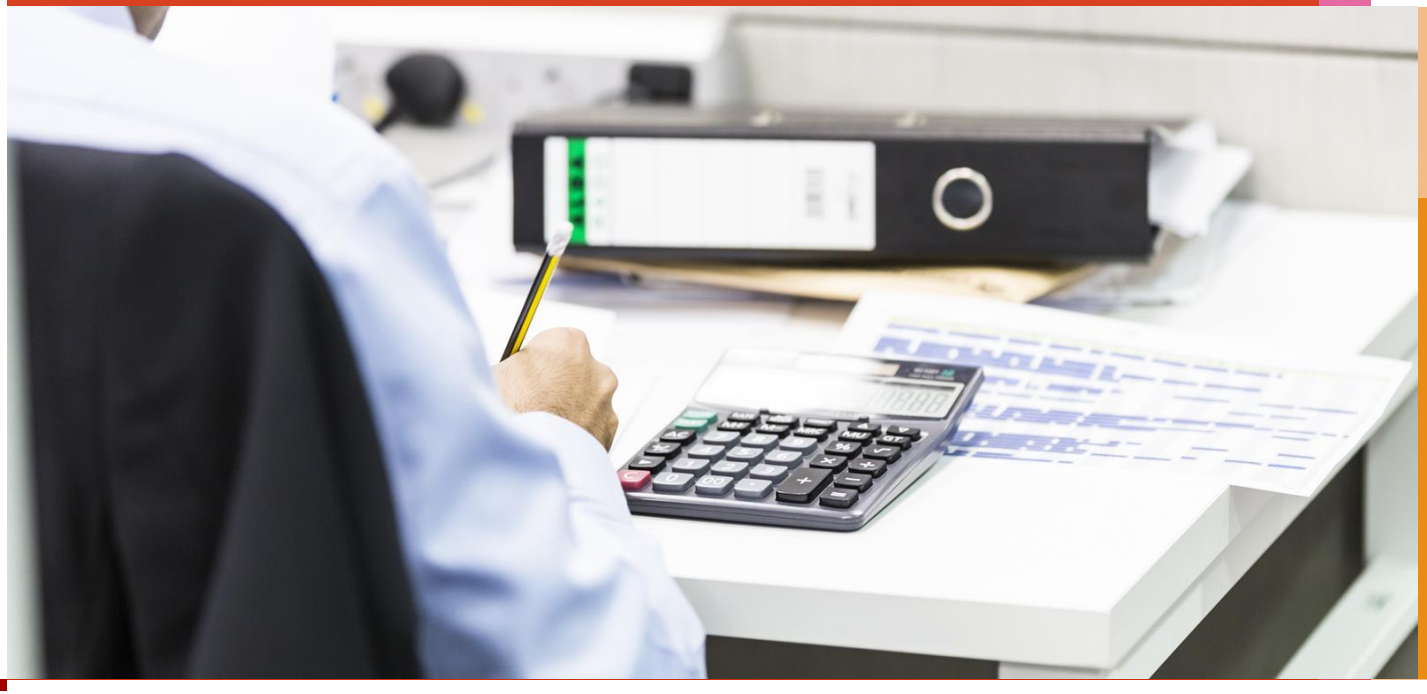
PwC CI Advisory

States of Guernsey

EU General Data Protection Regulation (GDPR) - High-level impact assessment

8 September 2016



pwc

Basis for this report

This document has been prepared only for the States of Guernsey and solely for the purpose and on the terms agreed with the States of Guernsey in our contract dated 6 June 2016.

We are providing no opinion, attestation or other form of assurance with respect to our work and we did not verify or audit any information provided to us.

We accept no liability (including for negligence) to anyone else in connection with this document.

Contents

To navigate this report on-screen (in pdf format)

From any page – click on the section title in the header navigation bar

From this Contents page – click on the title of the section or sub-section

From the contents listing on any section divider – click on the title of the sub-section

Background

The EU has come to an agreement on the introduction of the "General Data Protection Regulation" (GDPR) which will replace the current data protection legal framework originally developed in 1995.

The GDPR will apply from 25 May 2018, centralising regulation across the 28 member states of the European Union and updating Data Protection for the digital age. Any organisation processing personal data of data subjects in the EU for specific activities will need to be compliant. This is a major overhaul of current legislation, and will cause significant disruption to how organisations store, manage and process personal data.

The aims of the GDPR are to:

1. Give data subjects an increased level of control over their data;
2. Improve the protection of personal data by ensuring that data controllers and processors are safe custodians of data by promoting behavioural change; and
3. Provide for enhanced oversight and supervision by increasing the powers of the regulators.

The two-year window, that Guernsey has to ensure that it responds appropriately to this new regulation, began in May 2016.

Whilst this means that significant time and resources will be required, the right response will support the continued growth of our existing economy and strategically position the island to further develop opportunities in the data sector.

Scope and approach

The States of Guernsey's (the States) recognised the significance of the GDPR. PwC was engaged by the States to identify the key points and general considerations from the GDPR and their impact.

A high-level assessment was performed which provided an understanding of the GDPR principles and highlights how the GDPR will impact the local public sector, key industries and the regulator.

Our assessment was based on a desk-top analysis of the requirements of the GDPR regulations. It also included limited research into current trends and how other regulatory environments are expected to develop.

Consultation was not required, however, where in our opinion it was appropriate to meet with government, regulatory or industry representatives, we have done this as part of PwC's investment in supporting the States and the island, in this important project.

This public report is a summary of our key findings from our research.

Limitations of scope

Our findings were intended to help inform the States' strategic response to the GDPR, however there are matters of concern and potential options that will require further detailed investigation before business cases and a specific legal and regulatory model can be designed.

Alongside the GDPR, the EU has issued a Directive 2016/680. This Directive sets out the processing of personal data by relevant authorities in relationship to criminal offences. This Directive overrides the GDPR in that regard. We have not assessed the impact of Directive 2016/680 in the scope of this report.

Executive summary

Key points

- GDPR will be effective from May 2018 and is unavoidable.
- The GDPR will have significant impact on industry, the public sector and on the regulatory model.
- The economic consequences of doing nothing are potentially significant as existing industries are threatened by the loss of Guernsey's current 'adequacy' status.
- An appropriate response could however attract new commercial industries/opportunities, for example, organisations managing health data.
- Maintaining 'adequacy' is therefore essential. An EU re-assessment of this status will take place within four years.
- It is important that operational adequacy can be demonstrated through an effective regulatory model –the testing of this will be more stringent, for example, a MoneyVal type equivalent assessment.
- A new regulatory model will therefore be required.
- A Channel Islands based regulatory function is likely to remain the most cost effective option.
- A risk based regulatory model which also leverages and works with other existing on-island regulatory functions could reduce some of the additional burden.
- Funding will be a challenge as commercial models have not been established, however working with other regulators to collect revenue and ensure compliance could enable some costs to be covered.
- Working practices and EU expectations will evolve during the implementation period. The response therefore needs to be flexible.
- The next steps include drafting the legislation, developing an appropriate regulatory framework and working with industry to implement.

Key findings

The GDPR is unavoidable

Guernsey's current data protection regime is based on an EU Directive issued in 1995 (the 1995 Directive) which was incorporated into the Data Protection (Bailiwick of Guernsey) Law 2001.

The GDPR is much wider in its scope then the 1995 directive that it replaces. Any organisations that are active in Europe will need to comply with the GDPR. This includes organisations with no establishment in the EU but which are processing personal data of individuals in the EU relating to the offering of goods or services to individuals in the EU or the monitoring of their behaviour.

Brexit will therefore have no impact as organisations based in third countries like Guernsey are caught regardless. As such Brexit will not remove the need for such organisations to implement the changes required by GDPR. Furthermore, it is anticipated that the UK (as a third country) will implement an equivalent regime post Brexit.

The GDPR will have significant impact

The GDPR will have a significant impact for organisations in both the public and commercial sectors. The key changes include:

(i) The GDPR gives data subjects an increased level of control over their information:

- Consent – where data is being processed on the basis of consent, the data subject's consent now needs to be explicit;
- Right to be forgotten – a data subject has the right to erase personal data that is incorrect or no longer relevant, including withdrawing consent; and
- Data portability – a data subject can request the transfer of their personal data from one service provider to another.

(ii) The GDPR improves the protections for personal data by ensuring that data controllers and processors are safe custodians of data through promoting behavioural change:

- Data protection by design - organisations will need to consider privacy at the outset and throughout the design of any new system, product, service or process;
- Privacy impact assessments - organisations will have to perform and document privacy risk assessments and privacy audits as a matter of course where the activity poses a specific privacy risk;
- Data Protection Officers (DPO) – public sector organisations will be compelled to appoint a DPO, as well as other organisations who are performing certain high risk activities;
- Extension of responsibilities to cover Data Processors (in addition to existing requirements for Data Controllers) - an entity processing information on behalf another organisation will now be directly liable under the GDPR for failure to meet certain obligations; and
- Compliance responsibilities – organisations will need to be able to provide evidence to prove they are complying with the law. This means having paperwork documenting what personal data is used by the organisation and how.

Key findings (continued)

The GDPR will have significant impact (continued)

(iii) The GDPR provides for enhanced supervision by increasing the powers of the regulators:

- Fines - up to the higher of EUR 20 million or 4% of the entity's annual worldwide turnover;
- Audits and inspections – regulators will have increased power for onsite inspections; and
- Mandatory breach disclosure – organisations will be required to report certain breaches within 72 hours to the regulators and in some circumstances, to the individuals affected.

The GDPR recognises that individuals have rights to:

- Enter into class actions; and
- Seek damages for distress as a result of breaches.

The GDPR also aims to clarify the types of data included in the definition of 'personal data', specifically that it will include location data and online identifiers. Additionally, the GDPR adds genetic and biometric data to the catalogue of data attributes considered sensitive and requiring special measures and increased protection.

Implications of doing nothing

Guernsey's existing data protection regime has been assessed and determined to be 'adequate' in relation to the 1995 Directive. This essentially puts Guernsey on a 'white-list' of third countries enabling organisations to make international transfers of personal data to and from the island without regulatory restrictions or requiring additional safeguards to be put in place.

Although the GDPR recognises existing adequacy decisions made under the 1995 Directive, it should be remembered that adequacy decisions are subject to ongoing review. The GDPR specifies that any adequacy decisions made under the GDPR will be re-assessed at least every four years.

The GDPR does not set out the specific timing of the review, how or by whom it is triggered. It is possible that a review could be initiated at any time from now onwards.

If Guernsey decides not to implement an equivalent regime or fails to obtain adequacy status under the GDPR, Guernsey will be named by the EU Commission on a list of the third countries for which it has decided that 'an adequate level of protection is or is no longer ensured'. This will be published online and reported in the journal of the European Union. Hence while there would be no legal difference between Guernsey appearing on this list and another third country which has never been assessed, this list could be perceived as a 'black-list' and thus create uncertainty for business.

Thus whilst doing nothing is an option, this will be a significant threat to Guernsey's existing economy, for example the eGaming industry is very mobile and could quickly move to a jurisdiction which provides a lower impact regime.

Opportunities

Whilst the impact of the GDPR is unavoidable, an appropriate response could attract new commercial industries/opportunities, for example, organisations managing health data. These organisations may be looking for an enhanced regulatory environment, for example, certification seals.

Key findings (continued)

Operational adequacy is key

Under the GDPR, adequacy assessments will not just focus on the legal framework. It will be necessary for Guernsey to prove that the regulatory model is robust and operating in line with the requirements of the GDPR.

The GDPR goes into some detail about how the adequacy assessment will be performed. The practical details of this assessment process are not yet known, however we expect that future adequacy assessments will be much more rigorous and intrusive. This could be more similar to MoneyVal assessments, performed for AML purposes.

A new regulatory model is required

(i) Partial adequacy model

Guernsey could seek partial adequacy under the GDPR. For example, Canada is currently white-listed by the EU under the 1995 Directive, however their adequacy decision only applies to commercial organisations which are required to comply with relevant data protection legislation in Canada.

Canadian public sector organisations are dealt with under alternative legislation which has not been assessed for adequacy.

The GDPR allows for adequacy decisions to be made on a sector by sector basis and thus the partial adequacy model appears to be a potential option.

Whilst this initially seems attractive, any organisation that is caught under the GDPR by virtue of its processing activities will still have to apply the GDPR requirements even if that organisation is excluded under equivalent local legislation.

Most large organisations will want to apply a common set of processes across their organisation, however in the above instance, even if they operate to the higher standard, that organisation will not benefit from a territory level adequacy status. Thus they will have to deal with the commercial uncertainty and additional legal requirements for international transfers.

Partial adequacy is a feasible option that could be considered further, but it is only likely to benefit very restricted sectors which do not normally process EU personal data. In addition, it will result in multi-tier legislation, which will add complexity and potential confusion.

(ii) Full adequacy model

Under this model, Guernsey would enact new Data Protection legislation which mirrors the GDPR. The GDPR allows certain aspects of the legislation to be defined at a territory level, e.g. the age of a minor, however the legislation will be substantially the same.

Alongside the legislation, an enhanced regulatory approach will need to be developed. The role of supervisory authorities under the GDPR is crucial to monitor its correct implementation at the jurisdiction level.

We believe that there are opportunities for Guernsey to implement this new regulatory regime in an efficient, effective and economic manner, through a risk based approach.

Key findings (continued)

Supervisory authorities will be expected to have the powers, the legitimacy and the tools (including adequate budget, specialised staff and independence) to put all this in practice.

Funding

Establishing a new regulatory regime which meets the operational adequacy requirements set out in the GDPR will require significant additional resources to be available to the regulator.

At this time, no commercial models have been identified within the EU that generate regulatory income to fund these additional resources.

Consideration can be given to charging license fees, for example, on a tiered basis targeting organisations which are performing high risk data processing activity. However this could negatively impact Guernsey's competitive position if no other jurisdictions make a similar move. Working with other existing regulators and building the costs into existing regulatory fees could also reduce the overall impact.

Revenue could also be earned through other activities such as advisory or certification functions but it is possible that 'value added service' fees could be legally challenged as an impairment to the regulator's independence.

Building a business case based on potential regulatory fines is likely to be unworkable and undesirable to the commercial sector.

EU jurisdictions are likely to fund regulatory activities through state grants. Potentially, jurisdictions could then introduce a business levy to fund this grant.

We are, however, aware that other regulators are currently considering their funding mechanisms and thus whilst no public statements have been made, other jurisdictions may yet move to a more commercial licensing model.

A risk based approach, working with other regulators

As previously stated, the ability to prove operational adequacy will be key for Guernsey to maintain its full adequacy rating and the GDPR sets out the requirements for a supervisory authority that need to be met.

However, the GDPR does not set out the practical detail of how these requirements should be implemented.

The GDPR regulatory regime can be implemented with a risk based approach. This approach, for example, will allow the Data Protection Regulator to focus on organisations performing High Risk processing and to take comfort where other legislation and regulation contributes to the overall operational adequacy of the sector.

We consider that it will be most efficient and effective to continue the joint regulatory model working with Jersey. Particularly as many local businesses operate in both islands and want a common regulatory environment and standards.

Memorandums of Understanding (MOUs) could be established between existing local regulators, setting out how they will work together, to assist and avoid duplication of effort. This could include joint Commissioners working on Data Protection and other regulation i.e. financial services and eGaming. This joint cooperation would allow an element of regulatory activities to be funded via existing regulatory fee collection mechanisms.

Key findings (continued)

A risk based approach, working with other regulators (continued)

The feasibility of outsourcing aspects of the governance and oversight of the CI Data Protection Commission to the UK ICO could also be explored.

Similarly, organisations in the public and private sectors can adopt a risk based approach to the implementation of the requirements. Thereby focussing effort on those activities which are of highest risk or where organisations will benefit most from the strategic investment.

Next steps and key challenges

Government needs to:

- Set and communicate the overall strategy and direction, including the scope and regulatory objectives for Guernsey's new data protection regime.
- Work in conjunction with the Law Officers, to draft legislation and obtain the necessary approval.
- Ensure that the regulatory body is properly constituted, this includes appropriate governance and independence standards, which are currently not in place.
- Provide significant investment both in terms of financing, time and resources to build the new regulatory model which meets the required adequacy status.

Regulator needs to:

- Develop the regulatory model and activities which achieve the objectives set out in the overall strategy and regulatory objectives determined by Government. This regulatory model needs to be in place by the application date of the legislation and therefore needs to developed in parallel with the drafting of the legislation.
- Identify and obtain sufficient resources to implement the enhanced regulatory model. This will be a significant challenge, as the current CI Data Protection Commission only has sufficient resources to manage it's existing day to day responsibilities.
- Prepare for the EU adequacy assessment process, the timing and details of which are not yet known.
- Establish MOUs and any other relevant policies to work with other industry regulators and off island data protection authorities.

Public and commercial organisations need to:

- Determine the impact of the new regulation on themselves and implement the necessary changes to their systems and processes which ensure that they are compliant by the relevant application date.

Key challenges include:

- The GDPR does not provide for transitional arrangements, this means organisations have less than two years to implement the changes - this will be a significant challenge for many organisations.

Key findings (continued)

Key challenges (continued)

- For many organisations the GDPR is an evolution of existing data protection principles, however the new requirements will bring some specific challenges. The need to prove operational adequacy will also mean a new compliance journey with considerably greater responsibility to demonstrate how standards have been implemented. This means clearly designed processes supported by quality documentation, aligned with clear policies.
- It will be the responsibility of the Regulator to determine whether organisations are sufficiently compliant, including when and how regulatory inspections are performed.

Considerable clarification is still required

The GDPR has been eight years in the making and is the most lobbied piece of regulation in the history of the EU. However there are a considerable number of aspects of the regulation which are not clear in how they will operate in practice.

Whilst this is a potential opportunity for Guernsey to interpret and shape how our regulatory model is developed, it is inevitable that over the next two years and beyond, best practice and the expectations of the EU will continue to change.

It will therefore be necessary to have a flexible response and to monitor developments and respond to any changes that are identified to ensure that Guernsey's regulatory model continues to meet EU expectations.

Conclusion

Whilst the GDPR will introduce new obligations which will require additional investment in systems and resources across the public, commercial and regulatory sectors, we believe that there are significant economic threats if Guernsey does not maintain its adequacy status.

A pragmatic approach should be taken to the implementation of the regulation which achieves the GDPR requirements on a cost effective basis. This would involve a combination of risk based approach and a holistic view of where operational adequacy is achieved through other methods, for example, working carefully with other existing regulators.

However this will require careful planning and collaboration between government, regulatory bodies and industry.

Furthermore, this response supported by the right external promotion, will support Guernsey's strategic initiatives, such as 'Project Safehaven', and thus create new potential economic opportunities and possible efficiencies within the States of Guernsey's own operations.

Overview of the GDPR

High-level understanding of the GDPR

Introduction

The EU is introducing a new General Data Protection Regulation (GDPR) which will apply within the EU from 25 May 2018. The GDPR will replace the current framework based on an EU Directive issued in 1995 (the 1995 Directive).

The introduction of the GDPR has many significant changes in recognition of the change in volume and scope of data processing since 1995.

The GDPR will centralise regulation across the 28 member states of the European Union and updating it for the digital age. Any organisation targeting, monitoring or handling personal data relating to EU individuals will need to be compliant. This is a big shake-up, and will cause significant disruption to how organisations store, manage and process personal data.

Guernsey's current data protection regime

Guernsey's current data protection regime is the Data Protection (Bailiwick of Guernsey) Law 2001. This follows closely the UK Data Protection Act 1998 which is based on the 1995 Directive.

Guernsey's data protection regulation was assessed by the EU in 2003 and was determined to be adequate. This means that organisations can freely move personal data between the EU and Guernsey without putting in place additional regulatory requirements.

In 2012, Guernsey appointed a joint Channel Island Data Protection Commissioner to regulate Guernsey organisations in accordance with local legislation.

The GDPR is unavoidable

The GDPR is much wider in its scope then the 1995 directive that it replaces. Any organisations that are active in Europe will need to comply with the GDPR. This also includes those organisations with no establishment in the EU but which are directing goods and services at people in the EU or are collecting data on EU individuals.

This regulation is therefore extra-territorial in nature as it's remit covers all organisations who control or process personal data relating to European individuals, regardless of whether the organisation is based within or outside of the EU.

Brexit

The UK's referendum to leave the EU will have no impact, as set out above, organisations based in third countries are caught regardless.

It is likely that the GDPR will come into force in the UK during the exit period and it is expected on completion of negotiations, that the UK will implement an equivalent regime.

We have identified a risk that local organisations may be complacent with respect to the GDPR in the false belief that Brexit will change the local situation.

However, uncertainty in the UK caused by Brexit creates an opportunity for Guernsey. Positive and clear messages of the islands strategic intent in respect of the GDPR and political stability could generate additional opportunities.

Why does it matter to Guernsey?

Guernsey currently has an adequacy status as a third country

This adequacy or 'white-list' status means that transfers of personal data to that third country may take place without the need to obtain any further authorisation [Recital 103].

Guernsey organisations, particularly those in key industries such as Finance and eGaming, frequently transfer personal data to/from the Island and rely on this mechanism to do so.

If Guernsey loses its white-list status, the transfer of personal data would be prohibited, unless the requirements in the GDPR relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled [Recital 107].

The table on the right sets out these potential options. However in practice all of these would be extremely difficult to implement.

This will place additional burden and uncertainty on organisations and the likely outcome will be that businesses restructure their activities - resulting in a negative economic impact to the island.

Very few local organisations, as yet, have considered the consequences of Guernsey losing its white-list status.

Most are assuming that it will remain in place.

Options for transfers to a third country where no adequacy decision is in place

EU Model Clauses
The European Commission has established a standard set of clauses that a business can put in place as a basis to legitimately transfer data outside the EEA.

Binding Corporate Rules (BCRs)
BCRs are designed to allow multinational corporations, international organisations and groups of companies to make intra-organisational transfers of personal data across borders in compliance with EU data protection laws.

Privacy Shield
Until recently, transfers of personal data to the US were legitimised under the Safe Harbour regime. In October 2015 this regime was held invalid and a new framework – the EU-US Privacy Shield was adopted. It could be that a similar procedure is put in place for Guernsey which would involve the EU placing obligations on Guernsey companies to protect the personal data of EU data subjects and enable public authorities access to data.

Consent
Data can be transferred if a data controller has the consent of the data subject, however, obtaining, maintaining and adhering to the conditions of data subject consents can be an administratively burdensome task and consent will be harder to obtain under the GDPR.

Key elements of the new regulation - new data subject rights

One of the key drivers of the GDPR is to provide individuals with much greater rights over their personal data.

Consent

- Consent should be 'freely given, informed, specific and unambiguous'. The consent is to be received as a written declaration which is clearly distinguishable from other matters i.e. clear and affirmative.
- Data subjects also have the right to withdraw their consent at any time.
- Consent is required when the data is being processed for a new/different purpose.
- Consent is required from legal guardians to process data of minors.

Right to be forgotten

- The data subject can request the data controller to delete data entirely from the controller's system if (i) they withdraw consent and no legal grounds for processing remains, (ii) data is no longer required for purpose collected/processed, (iii) the data subject objects to processing or (iv) if processing does not otherwise comply with the GDPR.
- If information has been made public all links to information should also be deleted.
- This request should be carried out without undue delay and burdens the controller with the responsibility of removal of content held with third parties.

Data Portability

- The data subject has the right to request a copy of all of his or her electronically held personal data provided to a controller which then can be transmitted to another controller.
- The aim of this right is to allow data subjects to move between service providers without any loss of data and, therefore not requiring to re-input any information.
- The additional costs could be a big challenge for businesses.

Key elements of the new regulation – new accountability and operational adequacy requirements

The GDPR requires organisations to operate with greater transparency and accountability. In particular, there will be much greater onus on organisations to be able to prove operational adequacy through compliance activities.

Data protection by design	• Controllers must implement appropriate technical and organisational measures and procedures to ensure that processing safeguards the rights of the data subject by design. This includes consideration to (i) minimise data collected; (ii) not to retain that data beyond its original purpose; and, (iii) give the data subject access and ownership of that data.
Privacy impact assessments	• Data controllers must undertake privacy impact assessments where privacy breach risks are high to analyse and minimise the risks to their data subjects. • The GDPR sets out a list of processing operations that would constitute specific risks for this purpose, which includes: profiling; analysis of sensitive data relating to sex life, health, race and ethnic origin; and, large-scale CCTV monitoring of public places.
Data processors and third parties	• The responsibilities of the GDPR are extended to data processors as well as the controller. • Data controllers however retain their responsibility for personal data therefore organisations must carry out audits of third party processors for compliance with their data protection obligations. • Organisations must record and maintain a register of sensitive personal data shared with third parties.
Compliance responsibilities	• Organisations must demonstrate how they have complied with the regulation by providing quality documented evidence to support compliance. A failure to provide evidence will be deemed as non-compliance.
Data Protection Officer (DPO)	• A DPO needs to be appointed for all public authorities. It will also be required where the core activities of the data controller involves “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 and criminal convictions and offences.

Key elements of the new regulation – new regulatory powers and penalties

The GDPR also introduces requirements for regulators to have more enhanced investigation and enforcement powers.

Fines

- Fines made by the regulator of up-to the higher of €20 million or 4% of annual worldwide turnover. The risk of fines and penalties for entities process sensitive personal data is much greater.
- The regulator can impose a temporary or indefinite ban on processing and suspend data flows to a recipient in a third party.

Mandatory breach disclosures

- A data controller should inform the regulator of a data breach without undue delay within 72 hours after becoming aware of it. This should include what and how breach occurred and the effect and remedial actions to be taken.
- There is also a duty in some circumstances to disclose breaches to data subjects.
- There is a potential for brand damage with the disclosure of breaches and exposure to public embarrassment.

Litigation

- Data subjects can bring court proceedings where rights have been unduly infringed by damaging breaches.
- The GDPR recognises that individuals can join class actions and be entitled to damages for distress arising from a breach.

Article 75 of the General Data Protection Regulation states that:

"Every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation".

Article 77 goes on to state that:

"Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered".

Article 79 gives the power to the relevant Data Protection Authority to impose sanctions which:

"shall in each individual case be effective, proportionate and dissuasive".

Data protection timeline

GDPR

- The GDPR will apply from 25 May 2018.

States timeline

- A rough outline timeline for the update of the local data protection was initially prepared by the Committee for Economic Development.
- A detailed timeline is currently being prepared by the Home Department. This was not available for review but we were informed of key dates which are set out in the diagram.
- It is expected that the implementation date of the new Guernsey regulatory regime will be on or before that of the GDPR.

Key observations

- The initial timeline only considers the requirements to implement the legislative framework.
- Alongside the legal framework, a new regulatory framework needs to be developed. This includes constituting an appropriate regulatory body with the required governance and independence standards.
- Although the GDPR recognises existing adequacy decisions made under the 1995 Directive, the GDPR specifies that any adequacy decisions made under the GDPR will be re-assessed within four years.

  The GDPR does not set out the specific timing of this review, how or by whom it is triggered. It is possible that a review could be initiated at any time from now onwards.

Contacts

Nick Vermeulen
Partner

PricewaterhouseCoopers CI LLP
Royal Bank Place, 1 Glategny Esplanade, St Peter Port, Guernsey, GY1 4ND

Telephone: 01481 752089
e-mail: nick.vermeulen@gg.pwc.com

Jon Lowe
Senior manager

PricewaterhouseCoopers CI LLP
Royal Bank Place, 1 Glategny Esplanade, St Peter Port, Guernsey, GY1 4ND

Telephone: 01481 752028
e-mail: jon.lowe@gg.pwc.com