The Channel Islands Guide to the General Data Protection Regulation

CAREY OLSEN

9

Locations

5

Offshore Laws

BERMUDA
BRITISH VIRGIN ISLANDS
CAYMAN ISLANDS
GUERNSEY
JERSEY

1898

Founded

Contents

At Carey Olsen, we always look at the bigger picture. In the face of opportunities or challenges, our clients know that the advice and guidance they receive from us will be based on a complete understanding of their goals and objectives combined with outstanding client service, technical excellence and commercial insight.

BIGGER PICTURE

Background

Please note that this guide is currently being updated to incorporate the approval of the legislation since the guide was first published.

The GDPR – the view from the Channel Islands

This Guide addresses the Channel Islands issues which we have identified in relation to the new General Data Protection Regulation adopted last year by the European Union ("EU").

Whilst a great deal has been written about the subject in the UK, there has been little, if anything, which addresses the position of jurisdictions outside the EU.

This Guide is very much a summary of the most important issues that we have identified to date and is a work in progress. We will update it further as and when additional guidance is released and local legislation has been drafted.

Should you have any thoughts or questions regarding the issues set out in this Guide, please let us know - we are always delighted (and relieved) to discover others taking an interest.

If you would like legal advice in relation to any specific circumstances, please do give us a call.

What is the GDPR?

On 14 April 2016 the European Parliament voted to adopt the final draft of the new EU General Data Protection Regulation ("GDPR"), which updates and replaces the existing Data Protection Directive (95/46/EC) (the "Directive").

It represents the biggest shakeup in European data protection law in more than 20 years.

- The GDPR will replace the national data protection legislation in the various EU Member States (such as the Data Protection Act 1998 in the UK).
- Applies to "controllers" and "processors" of "personal data".

When does it go live?

The provisions of the General Data Protection Regulation already apply in all EU Member States, but will be enforced from 25 May 2018.

☑ To do

- Track guidance from EU, UK and local regulators
- Ensure internal training and awareness exercises are undertaken
- Make sure that decision makers and key people in your organisation are aware that the law is changing and appreciate the impact
- Consider resourcing/advisory requirements – there is likely to be significant competition for scarce expertise

Why does the GDPR matter in the Channel Islands?

Both Jersey (under the Data Protection (Jersey) Law 2005) and Guernsey (under the Data Protection (Bailiwick of Guernsey) Law 2001) were assessed as providing "adequate" levels of protection for personal data for the purposes of the Directive.

These adequacy decisions will continue to remain in force until they are formally reviewed (likely to be prior to 2020). After that, the Channel Islands may find it difficult to provide financial and other services to EU citizens and businesses unless their data protection regimes remain in line with EU requirements.

More importantly, the GDPR has significant extra territorial effect. Whilst the GDPR primarily applies to businesses in the EU, it will also apply to:

- Non-EU headquartered organisations "established" (see below) within the EU (for example, a company with a branch office or agent operating in London or Madrid), regardless of whether the organisation chooses to process data about EU individuals inside or outside the EU.
- Non-EU established organisations which are:
  a. offering goods or services to individuals who are in the EU, even if provided free of charge; or
  b. monitoring the behaviour of individuals who are in the EU, where their behaviour takes place in the EU.

The non-EU businesses which fall into the above categories will need to appoint a representative in the EU, subject to certain limited exemptions. The representative may have to accept liability for breaches of the GDPR and will be required to have authority to represent the business in cooperating with EU regulators to ensure compliance.

Even if the GDPR does not apply directly, both Jersey and Guernsey have announced their intention to enact legislation which will enable them to obtain an updated adequacy finding – meaning that local legislation will require broadly equivalent standards to those in force within the EU.

It is not clear whether Channel Islands businesses will nevertheless be required to designate a representative within the EU, given we will be operating under similar legislative frameworks. For businesses with a UK operation, but no other presence, or no EU presence at all, this is of particular concern. We will provide an update on this issue in due course.

☑ To do

- Determine if your business (if established outside the EU) is nonetheless caught by the GDPR
- Track changes to Channel Islands legislation
- Establish which law will apply (GDPR/new Channel Islands laws or both)

What about Brexit?

The UK has given notice of its intention to withdraw from the EU, which then starts a two year period in which the UK and the EU negotiate the terms of withdrawal.

On the basis of that timetable, the UK will still be in the EU when enforcement of the GDPR commences.

The UK Government has confirmed that the UK will implement GDPR and envisages maintaining similar legislation post-Brexit.

The Secretary of State Karen Bradley MP told the Culture, Media and Sports Select Committee:

> *"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."*

The UK Great Repeal Bill (when it becomes UK law) will likely transpose GDPR into UK law post-Brexit.

The UK Prime Minister Theresa May has stated:

> *"We seek a new and equal partnership between an independent, self-governing, global Britain and our friends and allies in the EU, ... But it is not partial membership of the EU, associate membership or anything that leaves us half in, half out. We do not seek to adopt a model already enjoyed by other countries. We do not seek to hold on to bits of membership as we leave."*

Once the UK leaves the EU, the applicability of the GDPR will depend on what type of Brexit deal the UK negotiates. Possibilities include:

- The UK remaining within the EEA and accepting the GDPR as part of membership of that organisation;
- The UK doing a deal which includes acceptance of the GDPR;
- The UK ending up outside the EEA but applying for an adequacy finding on the basis of its data protection legislation; or
- The UK deciding to do something different (for example in concert with the USA).

The above may have a significant impact on the applicability of the GDPR to businesses in the Channel Islands – particularly if most clients/data subjects are in the UK (although this will not alter the applicability of the homegrown GDPR legislation proposed in both Jersey and Guernsey).

There is a significant chance that controllers and processors in Jersey and Guernsey will need to cope with a number of related but distinct requirements depending upon where they are active and where their data subjects reside. The worst case scenario is that a Channel Islands controller/processor may need to cope with:

- The GDPR itself;
- National variations in relation to each EU jurisdiction to which they provide services; and
- Local Jersey/Guernsey data protection law.

☑ To do

- Track on-going Brexit developments
- Track on-going development of Jersey/Guernsey legislation
- Consider status of UK establishment/representatives post Brexit
- In any event, prepare for GDPR standards being applied in Channel Islands

Is it all new?

Existing data protection legislation in the Channel Islands is based on the UK Data Protection Act 1998, which is in turn based on the Directive.

Both Jersey and Guernsey have obtained adequacy findings from the European Commission in relation to their existing data protection regimes.

The GDPR retains the same core rules and principles for processing as the Directive and continues to regulate the processing of personal data only.

The definition of personal data is retained but extended to specifically include online identifiers, which can be IP addresses (including dynamic IP addresses), cookies or other identifiers such as radio frequency identification tags. This will remove some previous doubt as to whether online identifiers should be qualified as "personal data".

It is confirmed that "pseudonymous data" (broadly data which has been subject to internal anonymisation within an organisation) is considered personal data.

"Sensitive personal data" becomes "special category" data and its classes of data within its scope are extended to include genetic and biometric data. It may also become much harder to process information about criminal offences in some Member States.

All processing must comply with six general principles and must then satisfy a processing condition (see General Principles and Processing Conditions below). Whilst this mechanism is mostly familiar, there are some significant changes.

In particular, consent will be far more difficult to rely upon in practice (see below).

However, away from the basic mechanics of the GDPR, there are some major changes.

Sanctions and powers

The big headline in relation to the GDPR relates to the potential sanctions. Supervisory authorities will be able to issue fines of up to 4% of annual worldwide turnover (of the Group where appropriate) or €20 million (whichever is the greater).

Supervisory authorities have a wide range of other powers including:

- Auditing controllers and processors;
- Issuing warnings; and
- Imposing temporary and permanent bans on processing.

It is unclear as to how such powers are likely to work in relation to controllers and processors outside the EU, for example in the Channel Islands. The likelihood is that supervisory authorities within the EU will attempt to exercise such powers in relation to controllers and processors wherever they are based. Establishing an appropriate designated "representative" within the EU will therefore become highly important.

☑ To do

- Review commercial risk profile and insurance
- Assign appropriate resources to data protection issues
- Consider Group level response (and associated resourcing) in relation to GDPR issues

So a regulation means one law across the EU?

Sort of. In reality, the GDPR contains significant scope for Member States to amend and/or extend certain of its key terms, in particular:

- **Data protection officers** – Member States can make the appointment of a data protection officer mandatory as (for example) Germany does now.
- **Rules for the deceased** – the provisions of the GDPR only apply to data relating to living persons. However, the way is opened for Member States to regulate data relating to the deceased.
- **Employment** – Members States can introduce specific rules on the processing of employee data.
- **National security** – Member States can pass laws to limit rights under the Regulation in areas such as national security, crime and judicial proceedings.
- **Freedom of information** – Member States can amend the GDPR provisions to reconcile data protection with freedom of information, to protect information subject to professional secrecy and to restrict the processing of national identity numbers.
- **Children** – Member States can reduce the age at which a child can provide valid consent online from 16 to 13 years old.

Additionally, many processing activities are specifically dependent upon national laws in Member States. For example:

- **Processing conditions** – processing personal data can be justified where it is in compliance with an obligation under Union or Member State law.
- **Criminal offences** – the processing of information about criminal offences is only permitted where authorised by Union or Member State law (or where it occurs under the control of an official authority).

These national derogations and the interaction with other Member States' laws means the effects will not be fully harmonised across the Union and also call into question how the GDPR will interact with third country law (whether or not they are currently designated as "adequate").

Establishments, representatives and supervisory bodies

Establishment

The rules on whether a controller or a processor is established in the EU are complex – and likely to be made yet more complex by Brexit.

The GDPR will apply to organisations which have EU "establishments", where personal data are processed "in the context of the activities" of such an establishment. If this test is met, the GDPR applies, irrespective of whether the actual data processing takes place in the EU or not.

The definition of "establishment" was considered by the European Court of Justice ("ECJ") in the case of *Weltimmo v NAIH (C-230/14)* in the context of an online property portal. This case confirmed that the concept of an establishment is both broad and flexible in nature – the ECJ ruled that it may be sufficient if, through "stable arrangements" in the territory of a member state, the controller exercises a real and effective activity, even if this is minimal, in the context of processing personal data.

The presence of a single representative may be sufficient, although the guidance issued by the Article 29 Working Party in December 2016 in relation to identifying lead authorities (at 1 (v)) suggests that whilst this may be sufficient for enforcement purposes (and in particular the requirement to have a representative within the Union under Regulation 27 of the GDPR), it will not be sufficient to enable the business to take advantage of the "one stop shop" mechanism. This could result in businesses facing regulatory action from numerous supervisory authorities.

Additionally, organisations with have EU sales offices, which promote or sell advertising or marketing targeting EU residents, will likely be subject to the GDPR since the associated processing of personal data is considered to be "inextricably linked" to and thus carried out "in the context of the activities of" those EU establishments *(Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12))*.

Brexit may complicate matters – non EU data controllers may begin the life of the GDPR as established within the EU and then (once the UK leaves) have to appoint a representative in the "remainder" EU.

Representatives

A controller or processor which is not established in the EU, but which nonetheless is caught by the extra-territorial provisions of the GDPR, must appoint a representative. The representative must be based in a Member State in which the relevant data subjects are based. There is a limited exemption to the obligation to appoint a representative where:

- The processing is occasional and unlikely to be a risk to individuals; or
- Does not involve large scale processing of sensitive personal data.

This is potentially a very onerous role to accept. The representative will have to deal with relevant supervisory authorities and accept liability for breach of the GDPR.

Supervisory authorities

There will be a regulator in every Member State, known as a supervisory authority. The supervisory authority must be independent of the Member State.

There will also be a European Data Protection Board ("the Board"), made up of one representative from the supervisory authorities from each Member State.

The Board will take over from the current representative body, the Article 29 Working Party, but will have a much stronger role in providing guidance and co-ordinating enforcement of the GDPR through a consistency mechanism.

The one stop shop

The initial proposal was for a "one stop shop" regulatory mechanism under which businesses would only have to deal with a single supervisory authority for all processing carried out in the Union.

These proposals have been watered down and now only apply to cross-border processing – defined in the GDPR as meaning either:

- Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union, where the controller or processor is established in more than one Member State; or
- Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Following guidance from the Article 29 Working Party, the provisions are now likely to operate as follows:

- A business that carries out cross-border processing should be primarily regulated by the supervisory authority in which it has its main establishment (the lead supervisory authority).
- The guidance makes clear that this does not permit forum shopping and controllers must be able to demonstrate that "effective and real exercise of management activities takes place that determine the main decisions as to the purposes and means of processing".
- The burden of proof is on the controller or processor to prove this to supervisory authorities. Factors which may be taken into account in determining a main establishment include:
  a. where are decisions about the purposes and means of the processing given final 'sign off'?
  b. where are decisions about business activities that involve data processing made?
  c. where does the power to have decisions implemented effectively lie?
  d. where is the Director (or Directors) with overall management responsibility for the cross-border processing located?
  e. where is the controller or processor registered as a company, if in a single territory?
- The rules on the lead supervisory authority and the one stop shop mechanism do not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the supervisory authority of the Member State where the public authority or private body is established will exercise jurisdiction.
- A local supervisory authority can ask for control where the matter relates only to an establishment in its Member State or substantially affects individuals only in its Member State.
- The lead supervisory authority can refuse that request but must co-ordinate its activities closely with "concerned" supervisory authorities. If the other supervisory authorities object to the approach taken by the lead authority, they can ask the Board to override that decision.
- If a controller/processor does not have an establishment within the EU, the mere presence of a representative will not trigger the "one stop shop" and controllers without any EU establishment will need to deal with local supervisory authorities in every Member State in which they are active – although the effect of adequacy on this analysis is yet to be seen.

☑ To do

- Consider whether your business has an establishment within the EU
- Consider which EU territories your business is active in – can you identify a lead supervisory authority?
- Consider the practical requirements – what procedures, contractual arrangements, indemnities and the like are required?

General principles and processing conditions

The data protection principles are broadly the same as the existing regime. All processing must comply with six general principles:

- **Lawfulness, fairness and transparency** - personal data must be processed lawfully, fairly and in a transparent manner;
- **Purpose limitation** - personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- **Data minimisation** - personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **Accuracy** – personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- **Storage limitation** – personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (subject to exceptions for archiving); and
- **Integrity and confidentiality** – personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Processing must then satisfy a processing condition:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject. Only legal obligations under Union or Member State law will satisfy this condition. However, the obligation need not be statutory (e.g. common law obligations are sufficient);
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of (Member States or EU Law) official authority vested in the controller; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Public authorities may not rely on this condition.

Processing of sensitive personal data (or "special category" data) must then satisfy an additional processing condition:

- The data subject has given explicit consent;
- The processing is necessary for a legal obligation in the field of employment and social security law or for a collective agreement;
- The processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- The processing is carried out in the course of the legitimate activities of a not-for-profit body, only relates to members or related persons and the personal data is not disclosed outside that body without consent;
- The processing relates to personal data which is made public by the data subject;
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law;
- The processing is necessary for healthcare purposes and is subject to suitable safeguards;
- The processing is necessary for public health purposes and is based on Union or Member State law; or
- The processing is necessary for archiving, scientific or historical research purposes or statistical purposes and is based on Union or Member State law.

☑ To do

Consider:

- What personal data you collect
- Why you are processing it
- The legal basis for that processing
- Mapping data flows and risk assessing those flows to identify potential issues and areas for focus
- Develop processes and procedures to ensure compliance

Consent

The rules around consent have always been difficult to interpret under the Directive. The GDPR arguably does little to improve the position. The revised requirements make consent significantly more difficult to rely upon.

"Consent" is defined in the GDPR as "a freely given, specific, informed and unambiguous indication of the individual's wishes". Consent may be given by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing privacy settings, or another statement or conduct which clearly indicates acceptance of the proposed processing.

The GDPR imposes a number of conditions on consent – in particular:

- A request for consent must be in an intelligible and accessible form in clear and plain language;
- Where the request for consent is part of a written form which also concerns other matters, the request for consent must be clearly distinguishable from other matters;
- The consent must consist of a clear affirmative act. Inactivity or silence is not enough and the use of "pre-ticked boxes" is not permitted;
- Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. In practice this provision is likely to create challenges, since it is not immediately apparent whether ancillary processing (such as client communication) will require separate consents or be covered by "core" consent;
- Consent will not be valid if the individual does not have a genuine free choice or if there is a detriment if they refuse or withdraw consent;
- Consent might not be valid if there is a clear imbalance of power between the individual and the controller, particularly where the controller is a public authority. This will also be an issue in connection with employment.

Consent is presumed not to be freely given if:

- It does not allow separate consent to be given to different personal data processing operations (i.e. consent cannot be "bundled"); or
- If the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance (e.g. marketing/ advertising consent).

Consent must be capable of being withdrawn at any time and the data subject must be told of that right prior to giving consent. It should be as easy to withdraw consent as it is to give it (i.e. requiring an emailed response or requiring several "click-throughs" to confirm withdrawal will not be acceptable).

Finally, consent must be explicit if:

- Sensitive personal data ("special category data") is being processed; or
- Personal data is being transferred outside of the European Union.

☑ To do

- Consider what consents you rely on (if any) and whether they will continue to be effective
- Consider if you can rely on an alternative basis for processing (e.g. legitimate interests)
- Consider processes for obtaining consent in future, including revisions to websites, terms and conditions, clarity and simplicity of language

Data Protection Officers ("DPO")

Controllers and processors may be obliged to appoint a DPO where the following takes place:

- Processing is carried out by a public authority;
- Core activities of the controller or processor involve regular and systematic monitoring of individuals on a large scale;
- Large scale processing takes place of sensitive data ("special category data") or criminal records; or
- A Member State's law requires a DPO to be appointed.

There is limited guidance as to what "large scale" means, however it is noted that the Article 29 Working Party guidance refers to "considerable amount of personal data" affecting a "large number of data subjects" and "which are likely to result in a high risk". The parameters will develop with time, as more cases are assessed, however, it is important to bear in mind the context – processing the personal data of 80% of the population of a small Island may be seen as "large scale", whereas the same number of data subjects' records in a country the size of China may not be viewed in the same light, for example.

The role of the DPO is an important one and requires them:

- To inform and advise the controller or the processor and the employees who carry out processing of their GDPR obligations;
- To monitor compliance with the GDPR and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- To provide advice where requested as regards the data protection impact assessment and monitor its performance;
- To cooperate with the supervisory authority; and
- To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The GDPR requires the DPO to adopt a risk-based approach to his/her role.

The Article 29 Working Party has recently published guidance in relation to these requirements which provides as follows:

- **Public authority** – the guidance says that each Member State's laws should define what constitutes a public authority, and also that bodies which are subject to public law together with private organisations carrying out public tasks or exercising public authority should also fall within this definition. Assuming that the Channel Islands follow suit, most States departments and entities are likely to require a DPO;
- **Core activities** – activities which are "key operations necessary to achieve the controller's or processor's goals" are cited. Standard IT support activities and the processing of staff data do not appear to be included within "core activities". Examples of core activities given include:
  a. a security company's surveillance of public spaces;
  b. a hospital's processing of patient health data; and
  c. an outsourced provider of occupational health services processing of employee data.
- **Regular and systematic monitoring** – on-line tracking and profiling are cited as examples, including for the purpose of behavioural advertising and email retargeting. Other examples cited include:
  a. risk assessment scoring (e.g. for credit scoring, fraud prevention or the detection of money laundering);
  b. location tracking;
  c. fitness and health data tracking; and
  d. CCTV; and processing by connected devices (smart meters, smart cars, etc.).
- **Large scale** – the guidance does not specify what it means by "large scale" (although it suggests that some thresholds will be forthcoming). The following are suggested as factors to consider when assessing whether processing is "large scale":
  a. the number of data subjects concerned – either as a specific number or as a proportion of the relevant population;
  b. volume of data and/or the range of different data items being processed;
  c. the duration, or permanence, of the data processing activity; and
  d. the geographical extent of the processing activity.

Examples of large scale processing cited include:

- A bank or insurance company processing customer data; processing of an international fast food chain's customer geo-location data in real time for statistical purposes by a specialist processor;
- The DPO must be involved in all data protection issues and cannot be dismissed or penalised for performing their role;
- DPOs must have expertise and experience appropriate to their role;
- The DPO must report directly to the highest level of management within their organisation;
- A group of undertakings can appoint a single DPO. However, that data protection officer must be accessible to each undertaking and must have expert knowledge of data protection law and practice in the jurisdictions where the controller/processor is based – making a group appointment more difficult;
- DPOs must be able to speak the language of the country where the relevant controller or processor is based, so that they can communicate efficiently with data subjects and supervisory authorities. This may make it more difficult to appoint a centralised DPO for a group of companies;
- The GDPR allows DPOs to have other roles within an organisation, but this must not "result in a conflict of interest". The Article 29 Working Party guidance now expressly states that as a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of human resources or head of IT departments). It can also include other roles lower down the organisational structure, if such positions or roles lead to the determination of purposes and means of processing. Senior compliance roles are also arguably likely to conflict with the role and obligations of a DPO;
- DPOs may be provided by third parties on a service contract basis, but must have full powers and access and such arrangements must not result in a conflict of interest;
- The guidance encourages voluntary adoption of DPOs, but makes it clear that where an organisation adopts a DPO on a voluntary basis, they are subject to the same obligations and protections as mandatory DPOs. Where non-statutory data protection roles are to be created, they should be called something other than "data protection officer"; and
- Where a decision is made not to adopt a DPO, the reasons for this should be recorded.

The upshot of the above is that almost any financial services entity of any size in the Channel Islands with clients or customers in the EU is likely to have to consider appointing a DPO – either on a mandatory or voluntary basis. It remains to be seen whether this becomes a requirement of the local legislation in respect of any non-EU business.

☑ To do

Consider:

- Whether you are compelled to appoint a DPO
- If not, whether you wish to appoint a DPO on a voluntary basis
- If you do not appoint a DPO, who will "lead" data protection?
- Think about recruitment early – skills are likely to be in high demand
- If you are part of a group, could you have a group wide DPO or DPO team?
- Think also about delivery/project teams – if the DPO is the monitoring/awareness function, who will deliver the changes required?

Data security

The GDPR contains the same broad security obligation as the Directive, requiring controllers and processors to take appropriate technical and organisational measures to protect their systems.

This basic obligation is supplemented by a range of duties which include the following:

- Evaluating the risks of processing; and
- Implementing technical and organisational measures to mitigate those risks which take into account:
  a. the "state of the art";
  b. the costs of implementation; and
  c. the nature, scope, context and purposes of processing.

Businesses should adopt technical and organisational measures designed to ensure a level of security appropriate to the risk, include as appropriate:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

There is also a duty to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

It is notable that the above requires a risk based approach to be taken by controllers and processor – something which will be familiar to financial services entities.

Processors may find it difficult to undertake detailed risk assessment effectively, particularly where they are delivering commoditised services such as business continuity or cloud services. Accordingly, processors may need to plan for "worst case" scenarios and to ensure that pre contract due diligence is undertaken appropriately.

In designing compliance systems, controllers must also incorporate two new key concepts:

- **Data protection by design** – building in appropriate technical and organisational measures (such as pseudonymisation) at the design stage, which are designed to implement data-protection principles, such as data minimisation (in other words, thinking about the data protection implications at the outset and engaging with the relevant parts of the business); and
- **Data protection by default** – maintaining (or introducing) appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

The obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

In particular, such measures shall ensure that by default personal data are not made accessible (without the individual's intervention) to an indefinite number of natural persons. In practice, this will primarily involve ensuring privacy "settings" are high by default.

Recital 78 provides in relation to data protection by design and default:

> *"In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."*

☑ To do

- Conduct a risk evaluation to identify (and record) the risks arising from data processing
- Review and update your security measures and policies and procedures in light of the increased security obligations in the GDPR
- Ensure processors with whom you do business are adhering to similar standards
- Ensure that your business considers data protection at an early stage of projects in order to deliver data protection by design and by default

Fair processing/privacy notices

The GDPR significantly extends the information which must be given to data subjects by controllers at the outset.

The information which notices must contain includes:

- The Data controller's identity and contact details (including of his representative and DPO (if applicable);
- The purpose(s) for which data is processed, including the legal basis for the processing; and
- If the legal basis is the "legitimate interests" of the data controller, what those "legitimate interests" are.

Where data is obtained from a third party:

- The categories of personal data processed; and
- The source of the data, unless the personal data originates from publicly available sources.

A list of the data subjects' rights (i.e. the right of access, to rectification, to erasure, to object to processing or to obtain the data, as well as the right to data portability).

The data subject's right to withdraw consent (if this is the basis for processing).

The recipient or categories of recipients to whom the data will be disclosed.

Any intention to transfer the data subject's personal data to a country outside the EU or international organisation and information about the safeguards applied to any such transfer.

The right for data subjects to lodge a complaint with a supervisory authority and its contacts details.

If the data processing is a statutory/contractual requirement, whether the data subject is obliged to provide the data on that basis and the possible consequences of failure to provide the data.

Details of any automated decision-making, including details of the logic used and potential consequences for the individual.

Information about the existence of any profiling undertaken based on the data and its effects.

Any further information which is necessary to guarantee fair processing, having regard to any relevant code of conduct or relevant guidance (and specifying any high risk processing activities).

The notice must be provided:

- In an intelligible and easily accessible form; and
- Using clear and plain language.
- In writing and, where appropriate, electronically.

There are also specific rules on when the notice must be provided:

- If the data is collected from the data subject, at the time it is obtained.
- If the data is not collected from the data subject:
  a. at the time it is collected, or within a reasonable period after collection and, in any event, within one month;
  b. if a communication with the data subject is envisaged, at the time of the first communication with the data subject; or
  c. if a transfer to another recipient is envisaged, at the time of the first transfer.

If personal data is obtained from a third party, there is no need to provide a privacy notice if:

- The individual already has the information;
- Providing the information would be impossible or involve disproportionate effort, particularly where the processing is for archiving, scientific or historical research purposes or statistical purposes;
- The obtaining or disclosure is pursuant to Union or Member State law and there are appropriate measures to protect the individual; or
- The information is subject to professional secrecy.

☑ To do

- Ensure that fair processing/privacy notices are updated to comply with the GDPR
- Consider how privacy and other information notices should be delivered
- Where data subjects may be less "obvious" (such as trust beneficiaries/potential beneficiaries), consider how fair processing/ privacy notices will be dealt with

Breach notification

In several data breach cases, it has become apparent that controllers and processors have taken a deliberate decision not to publicise what has happened. This will no longer be an option under the GDPR.

A "personal data breach" is defined in the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

There are two types of notifications which are potentially required:

- Personal data breaches must be notified to supervisory authorities within 72 hours (where feasible) of the controller becoming aware of it (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons). The data breach notification needs to:
  a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
  c. describe the likely consequences of the personal data breach; and
  d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- When the personal data breach is likely to "result in a high risk to the rights and freedoms of natural persons", controllers must notify the data subject "without undue delay" in clear and plain language.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

Records of data breaches need to be kept even where they do not result in notification.

☑ To do

- Ensure that processes and procedures are adopted to identify and manage data breach notification obligations
- Design, implement and test incident response plans

Data subjects' rights

The general rights of data subjects under the Directive are preserved and extended. Those rights include:

- Data subject access;
- The right to rectification (similar to the Directive);
- The right to challenge automated decision-making (similar to the Directive);
- The right to lodge a complaint to the supervisory authority;
- The right to bring legal proceedings as well as the right to compensation and damages;
- The right to erasure (the so-called "right to be forgotten");
- The right to data portability; and
- The right to restrict the processing of personal data.

Some of the key rights are dealt with in more detail below:

Subject access

The data subject will have the right to obtain from the data controller, on request, confirmation as to whether his/her personal data is being processed together with the following information:

- The purposes of processing;
- Information about recipients of the data, particularly recipients in third countries (i.e. outside Europe);
- Retention periods;
- The existence of the right to request rectification or erasure or to object to processing;
- The right to lodge a complaint with the supervisory authority;
- In cases of automated processing, details of profiling; and
- Information about sources of the data.

If the data subject makes the request in electronic form the information should be provided in an electronic format (unless otherwise requested).

The data controller must provide the information without undue delay and, at the latest, within one month of receipt of the request.

The period for response may be extended to three months if necessary, taking into account the complexity of the request and/or the number of requests.

If the data controller intends not to respond to the request, they must inform the data subject without delay (and within one month) of the reason and the possibility of lodging a complaint with the supervisory authority.

Information provided and actions taken should be free of charge.

If the requests are "manifestly unfounded and excessive", in particular because of repetition, the data controller may charge a reasonable fee (to cover administrative costs) or refuse to comply with the request.

Responses to data subjects must be concise, transparent, intelligible and in an easily accessible form, using clear and plain language.

Member States may also restrict subject access rights to address:

- Public and/or national security;
- The prevention, investigation, detection and prosecution of criminal offences;
- The exercise of regulatory functions; and
- The protection of the data subject or the rights and freedoms of others.

The right to erasure (or the right to be forgotten)

Data subjects have a limited right to the erasure of their personal data already under ECJ case law relating to the Directive.

The Regulation extends and formalises this right. Data subjects would have the right to demand the erasure of personal data relating to them in the following circumstances:

- The data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- The data subject withdraws consent to processing and there is no other legal ground for the processing of data;
- The data subject objects to the processing of personal data in the "legitimate interests" of the data controller or for direct marketing or research purposes;
- The processing of the data has been unlawful;
- The data controller has a legal obligation to erase the data; or
- The data have been collected in relation to the offering of online services to children.

The data controller must erase all data "without undue delay".

In addition, where the controller has been responsible for making the data public, the controller must also take reasonable steps to inform other data controllers that the individual has requested the erasure of copies of and links to the data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

The right is not absolute and it does not apply if it is necessary to process the data:

- To exercise the right to freedom of expression;
- To comply with a legal obligation;
- To perform a task in the public interest or related to public health;
- For scientific or research purposes; or
- In connection with legal claims.

The right to restrict processing

Data subjects have the right to demand that the data controller restricts processing of the data, rather than erase it, if requested by the individual in the following circumstances:

- Where the data subject contests the accuracy of the data (only for a period sufficient to provide the data controller with an opportunity to verify the accuracy of the data);
- Where the data controller no longer needs to process the data, but the data subject requires the data to be retained in connection with a legal claim; or
- Where the data subject argues that the processing is not in the data controller's legitimate interests, and time is needed to determine whether the interests of the data controller override those of the individual.

If the processing of data is "restricted" such personal data shall, with the exception of storage, only be processed:

- With the data subject's consent;
- For the establishment, exercise or defence of legal claims;
- For the protection of the rights of another natural or legal person; or
- For reasons of important public interest of the Union or of a Member State.

Data portability

Another much heralded right for individuals under the GDPR relates to data portability.

Individuals already have the right to obtain their personal data. The new right enables them to ask for such data in an interoperable and machine readable format.

The right:

- Only applies to personal data "provided to" the controller; and
- Only applies where the controller is processing personal data in reliance on the processing conditions of consent or performance of a contract and the processing is carried out by automated means.

The Article 29 Working Party has issued new guidance and FAQs in relation to this right.

The Guidance adopts a broad interpretation of the scope of the right of data portability, suggesting that the right includes data provided "knowingly and actively" by the data subject (e.g. completing an online form), and data "exhaust" generated by their activity (e.g. data generated by a smart meter). This latter category of data includes raw data collected by virtue of the use of the service or the device, but not inferred or derived data generated by the controller, such as data generated by the subsequent analysis of the data subject (e.g. a credit score or assessment). The personal data must actually concern the data subject – in other words, anonymous data is out of scope. However, pseudonymous data is within scope if it can be clearly linked to a data subject.

The right to data portability does not apply where the processing of personal data is not based on consent or contract, such as when the data processing is based on the legitimate interests of the data controller or is necessary for the performance of a task carried out in the public interest, or where the data controller must comply with a legal obligation. However, the Guidance suggests that it may be good practice to provide data subjects with a right to data portability in such cases anyway.

☑ To do

- Set up processes (and where appropriate teams) to capture, record and act on requests to exercise individual rights
- Consider the technical requirements and how easily such data could be "bundled" for onward transmission

Accountability

At the heart of the GDPR is the concept of accountability. Not only must businesses comply with the six data protection principles, they must be able to demonstrate compliance. This falls into three primary areas:

- Data Protection Officers (see above);
- Privacy Impact Assessments; and
- Record keeping.

Data Protection Impact Assessments ("DPIAS")

Conducting DPIAs is already arguably best practice under the existing regime – the UK ICO have published a full Code of Practice on the conduct of DPIAs and recommends their use in a variety of processing contexts.

The GDPR goes further than this and requires their use when processing is likely to result in a "high risk" to the rights and freedoms of natural persons. This includes:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or significantly affects indiviudals;
- Processing sensitive personal data on a large scale; and/or
- Systematic monitoring of a publicly accessible area on a large scale, for example, using CCTV or facial recognition technology.

Supervisory authorities may specify processing activities they consider as high risk (and not high risk).

Controllers must consult their DPO, where designated, when carrying out a DPIA.

The assessment must contain:

- A systematic description of the envisaged processing operations and the purposes of the processing including, where applicable, the legitimate interest pursued by the controller;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to individuals; and
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR.

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Where a DPIA indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities.

Bearing in mind the requirements of Data Protection by Design and Data Protection by Default, we suggest that notwithstanding any obligation under GDPR, DPIAs are embedded in the design and implementation of any new system or process which involves the processing of personal data. Not only will this avoid potential hurdles further down the implementation process, it will go some way to demonstrating a compliance culture should there be a regulatory investigation at a later date.

Record keeping

One of the key changes under the GDPR is an end to the notification requirement in relation to processing activities (and the associated annual notification payment).

However, the benefit of this concession is minor and likely to be overlooked by most businesses when the scope of the accountability principle becomes clear.

Under the new accountability rules contained within the GDPR, businesses must maintain records of their processing activities. Whilst there is an exemption for small businesses (those employing less than 250 employees), the scope of the exemption is limited – it does not apply when processing activities are risky, frequent or include sensitive personal data.

Controllers (and where applicable their representatives must maintain) must be able to produce records of:

- The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the DPO;
- The purposes of the processing;
- A description of the categories of data subjects and of the categories of personal data;

- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- Where applicable, transfers of personal data to a third country or an international organisation;
- Where possible, the envisaged time limits for erasure of the different categories of data;
- Where possible, a general description of the technical and organisational security measures adopted.

Each processor (and where applicable their representatives) must maintain and be able to produce records of:

- The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the DPO;
- The categories of processing carried out on behalf of each controller;
- Where applicable, transfers of personal data to a third country or an international organisation; and
- Where possible, a general description of the technical and organisational security measures adopted.

☑ To do

- Establish whether a DPIA needs to be produced
- Adopt appropriate processes for producing a DPIA and acting on its outcomes
- Review and update existing data protection policies, procedures and compliance arrangements
- Create and maintain appropriate records of data processing

Processors

The GDPR applies directly to data processors. This is a significant change and is likely to result in a wholesale review of processing arrangements and contracts. It may also have significant cost implications for both processors and their customers.

The GDPR stipulates that there will be joint liability between a data controller and a data processor in cases of unlawful data processing. Only where the data controller or data processor is able to prove that it is "not in any way" responsible for the event giving rise to the damage, is it exempted from liability.

Many of the primary duties under the GDPR apply to processors including:

- Appointing a representative (if outside the EU);
- Record keeping;
- Breach notification;
- Appointing a DPO (where applicable);
- Sanctions; and
- Transfer of personal data outside of the EU.

There are also significant new requirements for data processing agreements which (as before under the Directive) must be in writing and ensure that the processor:

- Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Takes all appropriate security measures;
- Only engages a sub-processor with controller consent;
- Ensures that any sub-processors are bound by restrictions on their ability to sub-contract;
- Assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights under the GDPR (including subject access, rectification, the right to be forgotten, data portability and others);
- Assists the controller in ensuring compliance with security and data breach obligations;
- At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies (unless Union or Member State law requires storage of the personal data); and
- Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Additionally, the processor must inform the controller if, in its opinion, the controller's instructions would breach Union or Member State law.

☑ To do

- Controllers should review processing arrangements and contracts
- Processors should also revise their agreements and consider the commercial consequences of the increased obligations under the GDPR, in particular considering pricing changes and/or liability apportionment

Transfers outside the Union

The GDPR leaves the rules on international transfer of personal data largely unchanged. However, probably as a result of the European Court of Justice's "Safe-Harbor" decision of 06 October 2015, the GDPR now provides for a mechanism for periodic review of any EU Commission adequacy decision (at least every four years). It also includes enforceable data subject rights and effective legal remedies for data subjects (including the right to claim compensation in the Union or the third country) in addition to other safeguards such as contractual clauses.

The GDPR (unlike the Directive) covers not just the initial transfer to a third country, but also onward transfers.

There are several "transfer gateways" including:

- Transfers on the basis of an adequacy decision; and
- Transfers made subject to "adequate safeguards", which may be derived from:
  a. a legally binding agreement between public authorities or bodies;
  b. binding corporate rules (agreements governing transfers made between organisations within a corporate group);
  c. standard data protection clauses in the form of template transfer clauses adopted by the Commission ("EU Model Clauses");
  d. standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
  e. compliance with an approved code of conduct approved by a supervisory authority;
  f. certification under an approved certification mechanism as provided for in the GDPR;
  g. contractual clauses agreed and authorised by the competent supervisory authority; or
  h. provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.
- Transfers may also be made where the transfer is:
  a. effected with the individual's informed consent;
  b. necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
  c. necessary for the performance of a contract made in the interests of the individual between the controller and another person;
  d. necessary for important reasons of public interest;
  e. Necessary for the establishment, exercise or defence of legal claims;
  f. necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
  g. made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).
- Minor transfers - There is also a new (and very narrow) "minor transfers" exemption, which is unlikely to be of much practical application.

It should be noted that many of the existing bases for transfer outside the European Union have been challenged – the US Safe Harbor has been struck down and its replacement (the so called "Privacy Shield") is also being scrutinised and will likely be subject to challenge. Additionally, whilst the GDPR appears to endorse Binding Corporate Rules, they have historically been regarded as unwieldy, costly and difficult to manage in anything other than a major group. This may change if the "one stop shop" approach proves to be effective.

☑ To do

- Consider data flows and identify any international transfers
- Review basis for international transfers
- Where consent is relied upon, consider whether an alternative basis would be better/ of more practical use

What next?

The Article 29 Working Party has published guidance relating to:

- The right to data portability;
- Data protection officers; and
- The lead supervisory authority.

Further guidance will be published and existing guidance augmented during 2017.

The Article 29 Working Party have announced that they are due to be undertaking the following work in 2017:

- Follow-up on 2016 – finalising work in relation to:
  a. certification;
  b. "High Risk" processing;
  c. Data Protection Impact Assessments;
  d. administrative fines;
  e. the setting up the European Data Protection Board (EDPB);
  f. the "one stop shop"; and
  g. the EDPB consistency mechanism.
- New 2017 priorities:
  a. guidelines on the topics of consent and profiling;
  b. guidelines on the issue of transparency; and
  c. updating existing opinions and guidance on data transfers to third countries and data breach notifications.

The UK Information Commissioner will continue to publish guidance.

Jersey and Guernsey are due to publish their proposed GDPR – compliant legislation in Summer 2017.

The GDPR comes into full effect on 25 May 2018.

Further guidance

The EU Commission's data protection homepage is at https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection_en

The UK Information Commissioner has published a range of data protection guidance which is likely to inform Channel Islands practices. This is available at https://ico.org.uk/

The Channel Islands Data Protection regulators can be accessed at https://dataci.org/

Any questions?

Please do not hesitate to contact us with questions or queries. We are happy to provide more bespoke training or guidance to your business on GDPR or specific areas of the legislation and happy to provide advice as required.

From an awareness viewpoint, we are more than happy to speak to boards and/or risk committees on the requirements.

Key contacts

For further information or professional advice please contact our lawyers below:

Mark Dunster
Partner, Guernsey

D +44 (0)1481 732015
E mark.dunster@careyolsen.com

Elaine Gray
Partner, Guernsey

D +44 (0)1481 732035
E elaine.gray@careyolsen.com

Carly Parrott
Counsel, Guernsey

D +44 (0)1481 741523
E carly.parrott@careyolsen.com

William Grace
Partner, Jersey

D +44 (0)1534 822361
E william.grace@careyolsen.com

Siobhan Riley
Partner, Jersey

D +44 (0)1534 822355
E siobhan.riley@careyolsen.com

Huw Thomas
Counsel, Jersey

D +44 (0)1534 822224
E huw.thomas@careyolsen.com

FIND US

Carey Olsen (Guernsey) LLP
PO Box 98
Carey House
Les Banques
St Peter Port
Guernsey GY1 4BZ
Channel Islands

T +44 (0)1481 727272
F +44 (0)1481 711052
E guernsey@careyolsen.com

47 Esplanade
St Helier
Jersey JE1 0BD
Channel Islands

T +44 (0)1534 888900
F +44 (0)1534 887744
E jerseyco@careyolsen.com

FOLLOW US

Visit our regulatory team at careyolsen.com

About us

Carey Olsen is a leading offshore law firm advising on the laws of Bermuda, the British Virgin Islands, the Cayman Islands, Guernsey and Jersey from a network of nine international offices.

We provide legal services in relation to all aspects of corporate and finance, trusts and private wealth, investment funds, insolvency, restructuring and dispute resolution.

Our clients include global financial institutions, investment funds, private equity and real estate houses, multinational corporations, public organisations, sovereign wealth funds, high net worth individuals, family offices, directors, trustees and private clients.

We work with leading onshore legal advisers on international transactions and cases involving our jurisdictions.

In the face of opportunities and challenges, our clients know that the advice and guidance they receive from us will be based on a complete understanding of their goals and objectives combined with consistently high levels of client service, technical excellence and commercial insight.

Cybersecurity and Data Protection

Whether you're compiling data protection processes, reviewing current practices or managing a claim we have a team of specialists who can advise you.

Carey Olsen is one of the only offshore law firms to offer focussed contentious and non-contentious data protection and information management services. Our experts advise clients on local legislation governing the collection, processing and storage of data on customers, staff and suppliers to achieve a secure data management framework that complies with the law.

Our clients are primarily financial services operations who instruct us because of our in-depth knowledge of financial services regulation. We also act for clients in the general commercial sector who appreciate our pragmatic, straightforward advice.


50+
Partners
200
Lawyers
200
People

Contact us

Jurisdictions

Bermuda

Carey Olsen Bermuda
2nd Floor
Atlantic House
11 Par-la-Ville Road
Hamilton HM11
Bermuda

T +1 441 542 4500
E bermuda@careyolsen.com

British Virgin Islands

Rodus Building
PO Box 3093
Road Town
Tortola VG1110
British Virgin Islands

T +1 284 394 4030
E bvi@careyolsen.com

Cayman Islands

PO Box 10008
Willow House
Cricket Square
Grand Cayman KY1-1001
Cayman Islands

T +1 345 749 2000
E cayman@careyolsen.com

Guernsey

Carey Olsen (Guernsey) LLP
PO Box 98
Carey House
Les Banques
St Peter Port
Guernsey GY1 4BZ
Channel Islands

T +44 (0)1481 727272
E guernsey@careyolsen.com

Jersey

47 Esplanade
St Helier
Jersey JE1 0BD
Channel Islands

T +44 (0)1534 888900
E jerseyco@careyolsen.com

International offices

Cape Town

Protea Place
40 Dreyer Street
Claremont
Cape Town 7708
South Africa

T +27 21 286 0026
E capetown@careyolsen.com

Hong Kong

Carey Olsen (Hong Kong) LLP
Suite 4120
Jardine House
1 Connaught Place
Hong Kong

T +852 3628 9000
E hongkong@careyolsen.com

London

Carey Olsen LLP
8-10 Throgmorton Avenue
London EC2N 2DL
United Kingdom

T +44 (0)20 7614 5610
E londonco@careyolsen.com

Singapore

Carey Olsen Singapore LLP
Level 11
Marina Bay Financial Centre
Tower 1
8 Marina Boulevard
Singapore 018981

T +65 6653 4330
E singapore@careyolsen.com