CAREY OLSEN

The transitional arrangements have ended – what next?

Service area / Cybersecurity and Data Protection
Location / Guernsey
Date / June 2019

On 25 May 2019 the Bailiwick of Guernsey's new data protection regime became fully operational. Following the end of the transitional arrangements which were established in May 2018 under the Data Protection (Bailiwick of Guernsey) Law, 2017 ("Law"), Leonie Corfield explores what this means for businesses in the Bailiwick.

The Law came into force on 25 May 2018. It was enacted in order to align the Bailiwick's data protection regime with that in place under the EU's General Data Protection Regulation ("GDPR"). However, unlike the GDPR the Law 'grandfathered' certain aspects of the previous data protection regime for one further year to allow businesses locally to prepare.

On 25 May 2019 the transitional relief largely came to an end with one exception, that we explain later. This means that any companies are fully in compliance with the Law.

The exception to this rule is that the States of Guernsey has passed a set of Regulations extending the transitional exemptions relating to registration and fees until 31st December 2019.

Registration and fees

Part of the challenge for jurisdictions across Europe has been determining how registration and fees should work; Guernsey is no exception to this. Whilst these issues are still being worked out, there is a transitional regime in place as follows:

- The registration process is simplified – local businesses are no longer required to submit reams of information to the ODPA relating to their processing activities and data transfers. The expectation is that this information must, instead, be documented as part of their record-keeping arrangements.
- Those entities under the law who were exempt from registration under the previous regime may continue to rely on this until 31 December 2019. These were businesses who were exempt: by virtue of either their charitable/not for profit or processor status or because they could rely on the exemption based on thier "core business purposes" being staff administration and marketing thier own good and services. They will, however, need to document their rationale for relying on the relevant exemption.
- The online register has been abolished and will no longer be publically accessible.

We understand that further guidance will be published by the ODPA in the coming months to clarify the new fees regime which will complement the registration process.

Privacy notices

Pre- 25 May 2019	Until 25 May 2019 a controller was exempt from the duty to notify data subjects in respect of the processing of personal data which was collected in the context of the controller prior to 25 May 2018.
Now	Controllers must ensure that compliant privacy notices have been sent to all those persons who are entitled to receive them. (Note the Law provides for certain exceptions to this duty in certain limited circumstances.)
Practical implications	Businesses should: • undertake reviews as to what personal data they hold and why; • establish the legal basis for which they collate and process data (bearing in mind that additional processing grounds have been published under secondary legislation); and • update their privacy notices as to how personal data is handled for circulation to data subjects whose personal data they hold.

Joint controllers

Pre- 25 May 2019	Until 25 May 2019 a controller was exempt from the requirement to comply with the duties of joint controllers in respect of personal data already held before 25 May 2018.
Now	All businesses are required to assess their arrangements with third parties to establish whether they are controllers, processors or joint controllers and document their rationale.
Practical implications	The Law requires two or more joint controllers to set up "arrangements" regarding their compliance with data subjects' rights. Joint controllers will need to decide who will carry out each relevant controller obligation. This has potentially wide implications for all businesses when determining their breach notification requirements as well as how and who should be responsible for complying with individuals' rights as, ultimately, each controller remains responsible for complying with all of the obligations of controllers. Joint controllers are not required to have a contract (although we would recommend this) but must have a transparent arrangement that sets out agreed roles and responsibilities. The main points of this arrangement should be made available to data subjects. The UK Information Commissioner's Office (ICO) recommends that this is included as part of the privacy information.

Data Privacy Impact Assessments ("DPIAs")

Pre- 25 May 2019	Until 25 May 2019, the duty to carry out DPIAs under sections 44 and 45 of the Law in respect of any high risk data processing underway before 25 May 2018 was suspended.
Now	Controllers are required to assess whether a DPIA needs to be carried out for "high risk processing".
Practical implications	If large amounts of sensitive personal data are processed or if, for example, systematic and extensive automated processing of personal data are conducted, a DPIA must be carried out.

Data processing agreements

Pre- 25 May 2019	Until 25 May 2019 controllers and processors were exempt from the requirement to update existing contracts with processor/controller provisions in respect of contractual arrangements in existence before 25 May 2018 (including compliance, by processors, of certain duties under section 35 Law).
Now	All services agreements/supply contracts and terms of business may need to be updated to comply with the data processor requirements as set out in the Law.
Practical implications	Controllers and processors should carefully consider their supply chain to establish whether their suppliers/service providers and other third parties are processors and/or sub-processors. If the answer is 'yes', then controllers should next review the terms of any existing service agreements to establish whether appropriate data processing terms need to be incorporated in accordance with the Law. The parties should also consider whether any contractual safeguards are required in the context of transfers of personal data to other entities outside of the Channel Islands/the European Economic Area (EEA).

Continued

Portability	
Pre- 25 May 2019	Until 25 May 2019 the right of data subjects to port data (i.e. to instruct an organisation to transfer or copy their data from that organisation's systems and provide it to them in a "machine readable" form for transfer to another IT system) was delayed.
Now	Controllers should be prepared to receive and handle porting requests from data subjects in addition to other requests, such as subject access.
Practical implications	The right of portability is a potentially costly exercise for the unwary. Controllers, when faced with a porting request, should assess what (if any) data the data subject is entitled to receive and ensure that information is appropriately delivered. Controllers should consider putting place appropriate policies and procedures to address this right (which should sit alongside a controller's policy on data subject access requests).

Consents	
Pre- 25 May 2019	The Law introduced more stringent requirements about the form of consent to be sought from data subjects where consent was the basis upon which the organisation relied in order to process relevant personal data. Where organisations were already processing personal data of an individual prior to 25 May 2018 and were relying on their consent to do so, another year was given to ascertain whether that consent needed to be updated and/or a valid consent obtained for the purposes of the Law.
Now	Ensure any data subject consents received in respect of personal data processing are obtained in a valid form for the purposes of the Law.
Practical implications	Controllers should first establish to what extent consent has been relied on in the past. Next assess whether consent is still appropriate in light of the requirements of the Law. Finally, to the extent that consent is still necessary, controllers should review their consent wording (and privacy notices) and update as necessary.

Public authorities	
Pre- 25 May 2019	Reliance by public authorities on legitimate interests as a lawful basis for processing was permitted until 25 May 2019.
Now	All public authorities should re-establish their basis for processing personal data now that legitimate interests basis has been abolished.
Practical implications	Public authorities should review their privacy notices and ensure that these have been updated accordingly.

For further assistance please contact a member of our cybersecurity and data protection team.

Continued

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
E guernsey@careyolsen.com

FOLLOW US

Subscribe for more

Visit our cybersecurity and data protection team at careyolsen.com

PLEASE NOTE