DATA PROTECTION LAWS OF THE WORLD

Guernsey

DLA PIPER

GUERNSEY

Last modified 31 January 2022

LAW

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("**DPL 2017**") came into force on 25 May 2018 to coincide with the enforcement of the EU's General Data Protection Regulation (EU) 2016/670 ("**GDPR**").

Adequacy

The DPL 2017 replaced Guernsey's first set of data protection legislation that was introduced in 2001 in the form of the Data Protection (Bailiwick of Guernsey) Law, 2001, as amended ("**DPL 2001**"). The DPL 2001 had been implemented in response to the EU Directive 95/46/EC. Whereas the DPL 2001 was modelled on a UK enactment, the DPL 2017 is stated to be 'equivalent' to the GDPR.

In 2003 Guernsey was recognised by the European Commission as providing an adequate level of protection for the free flow of personal data to the Bailiwick (see Opinion 02072/07/EN WP 141 and Opinion 10595/03/EN WP 79). Following the enforcement of the GDPR from 25 May 2018, the adequacy decision remains valid and effective in respect of Guernsey's revised data protection regime under the DPL 2017. The adequacy decision is currently being reassessed by the European Commission (as per Article 45(9) GDPR) and confirmation of the outcome of such reassessment was expected during 2021, but this is still awaited.

Scope and applicability

The DPL 2017 applies in relation to the processing of personal data where:

- the processing is by automated means (whether wholly or partly) **OR** if, the processing is not by automated means, it is intended to form part of a filing system; and
- the processing is conducted by a controller or processor established in the Bailiwick of Guernsey ("**Bailiwick**") **OR** the personal data is that of a Bailiwick resident and is processed in the context of the offering good or services (whether or not for payment) to the resident or the monitoring of the resident's behaviour in the Bailiwick. The term "established in the Bailiwick" is defined under the DPL 2017.

In practice, this means that there may be instances where controllers and processors established in the Bailiwick are subject to both the DPL 2017 and, where they process personal data of data subjects who are in the EU, the GDPR.

A domestic exception is available where the processing is for the purpose of an individual's personal, family or household affairs.

As from 25 May 2019, the initial period of transitional relief granted to controllers and processors in Guernsey came to an end. All controllers and processors must therefore comply with all aspects of the DPL 2017 (including the duty to notify pre-collected data, carry out privacy impact assessments, comply with statutory obligations in relation to processor and joint controller-led duties and renew consents collected prior to 25 May 2018).

There is also a requirement (in certain instances) for controllers not 'established in the Bailiwick' to designate and authorise a

representative in the Bailiwick.

DEFINITIONS

Definition of personal data

Section 111(1) of the DPL 2017 defines personal data as "*any information relating to an identified or identifiable individual*".

An 'identifiable individual' is given special meaning under Schedule 9 of the DPL 2017 and is defined as an individual who can be directly or indirectly identified from the information including:

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

Definition of special category data

'Special category data' means personal data consisting of information as to a data subject's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data, meaning personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about their physiology or their health, including as a result of an analysis of a biological sample from that individual
- biometric data, meaning personal data resulting from the specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data
- health data, which includes any personal data relating to the health of an individual, including the provision of health care services, which reveals their health status and includes information about their physical or mental health
- sex life or sexual orientation
- criminal data which relates to the commission or alleged commission by an individual of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Overall oversight of the implementation of the DPL 2017 is vested in the Data Protection Authority ("**Authority**"). The Authority delegates many of the day-to-day regulatory functions and provides governance to an independent operational body known as the Office of the Data Protection Authority ("**ODPA**") (formerly, the Office of the Data Protection Commissioner).

The Authority and the ODPA are also required, pursuant to The Data Protection (International Cooperation and Assistance) (Bailiwick of Guernsey) Regulations, 2018 to have regard to Articles 60 – 62 GDPR by providing mutual cooperation with other supervisory authorities relating to both the GDPR and the DPL 2017.

The office of the data protection authority

St Martin's House
Le Bordage

St. Peter Port
Guernsey
GY1 1BR

Telephone

+44 (0) 1481 742074

E-mail

enquiries@odpa.gg

Website

odpa.gg

REGISTRATION

Section 39 of the DPL 2017 prohibits all controllers **and** processors established in the Bailiwick from processing personal data unless they have registered with the ODPA. Failure to comply with section 39 of the DPL 2017 is a criminal offence.

The Authority may prescribe the form and manner of registration. These particulars are described in the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018 (as amended) (the "**Registration Regulations**")) which set out the framework for a new registration and levy collection regime applicable from 1 January 2021. The new regime abolishes the previous set of exemptions from registration (which expired on 31 December 2020) and replaces them with a much narrower sub-set of exemptions.

The Registration Regulations also introduce the concept of a 'Levy Collection Agent', which is, in essence, a regulated entity licensed by the Guernsey Financial Services Commission (GFSC) who has been appointed to collect an entity's registration fees on its behalf.

Importantly, whilst a Levy Collection Agent has certain responsibilities under the Registration Regulations (which include submitting an annual return, preparing and issuing certificates of exemption to all relevant entities which it administers and retaining records on such entities for a period of 6 years), the ODPA has clarified in its guidance that "*all the legal responsibility as well as liability for data protection compliance still rests with [the controller/processor]…[and in this regard Levy Collection Agents] are simply … a payment gateway to assist with the administrative requirements for the regulated community.*"

Exemptions

Certain limited exemptions to the requirement to register are available to some controllers and processors under the Registration Regulations. These include, for example, where the controller and/or processor has appointed a Levy Collection Agent on its behalf. Not all entities will be eligible to appoint a Levy Collection – this route is only available to organisations who employ fewer than 50 FTE employees, are not required by law to appoint a DPO, do not already act as a Levy Collection Agent and are not nonprofits.

If a controller or processor seeks to rely on any one exemption, they must document their rationale for their decision.

Registration particulars

Since the introduction of the DPL 2017, the ODPA has streamlined the registration regime, both from an outward-facing and internal perspective. For example, in accordance with the GDPR's approach, the register is no longer available to be searched online, thereby removing the requirement for the ODPA to maintain a public register containing significant volumes of processing details. The ODPA has also removed the requirement for controllers and processors to include details about the types of processing undertaken and no longer requires entities to provide a description of the categories of data subject or details of the countries to which such data is transferred.

Instead, at the time of writing, a controller or processor established in the Bailiwick who is required to register with the ODPA must give the ODPA an online annual return setting out the following information (as stipulated in the Registration Regulations):

- the contact details (including name and principal business address) of the entity to be registered
- confirmation of whether the entity is a controller, processor or both in relation to the processing activities
- the representative[1] appointed (if the entity is based outside the Bailiwick)
- confirmation of whether the entity is a charity / not-for-profit
- the DPO (as applicable)
- confirmation of whether the entity employs 50 or more full time equivalent employees
- confirmation of whether the entity has agreed to act as Levy Collection Agent

The return must also be accompanied by a levy, which will be calculated depending on the status of the organisation (i.e. if it is a charity/not for profit) and the number of full-time equivalent employees employed by the entity.

Levy Collection Agents are required to submit a slightly different set of information to the ODPA, as follows:

- the contact details (including name, principal business address and GFSC number) of Levy Collection Agent
- confirmation of whether the entity is a controller, processor or both in relation to the processing activities
- the DPO (as applicable)
- confirmation of whether the entity employs 50 or more full time equivalent employees
- Declaration of the number of organisations the Levy Collection Agent is acting for.

The return must also be accompanied by a levy (being the aggregate of its own fees plus those of the entities that it administers).

There are two levels of fees:

- For organisations with 1-49 full-time equivalent (FTE) employees - £50 per annum; or
- For organisations with 50 or more FTE employees - £2,000 per annum.

The Registration Regulations stipulate separate levies are applicable when dealing with certain government bodies.

---

1. Section 38 of the DPL 2017

DATA PROTECTION OFFICERS

A data protection officer (**"DPO"**) must be appointed where:

- processing is carried out by a public authority (other than a court, or tribunal acting in a judicial capacity); or
- the core processing operations of the controller or processor require or involve "*large-scale and systematic monitoring of data subjects*" or "*large-scale processing of special category of data*".

The ODPA has issued guidance clarifying what is intended by the use of the term "*large-scale processing*", noting that this term is not defined in either the GDPR or the DPL 2017.

The ODPA's guidance references the guidance on the appointment of DPOs ("**DPO Guidelines**") issued by the EU's former advisory body (previously known as the Article 29 Working Party and now replaced by the European Data Protection Board ("**EDPB**")). The ODPA advises controllers and processors to take into account the terms of both the GDPR and the DPO Guidelines when assessing whether or not a DPO is required to be appointed. It also clarifies that small businesses in Guernsey are, as a general rule, unlikely to be undertaking large-scale processing unless they work with large databases of customers or other types of data subjects. Finally, the ODPA expects controllers and processors to review the scope and nature of processing periodically to ascertain whether or not their prior assessment remains valid or if there are sufficient factors to warrant appointing a DPO. All controllers and processors should document their decision-making and the outcome of such reviews.

COLLECTION & PROCESSING

Principles

Data controllers must comply with the data protection principles set out under Section 6(2) DPL 2017 ("**Principles**").

The Principles comprise:

a. **Lawfulness, fairness and transparency**: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data
b. **Purpose limitation**: personal data must be collected for specified, explicit and legitimate purposes and, once collected, not further processed in a manner incompatible with those purposes
c. **Data minimisation**: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
d. **Accuracy**: personal data must be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
e. **Storage limitation**: personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed
f. **Integrity and confidentiality**: personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
g. **Accountability**: the controller is responsible for, and must be able to demonstrate compliance with, the data protection principles described under paragraphs (a) – (f) above.

Lawful basis

Data controllers are required to ensure that they have a lawful basis for processing personal data. The DPL 2017 sets out a number of conditions which may be relied upon to legitimise the processing of personal data and special category data.

The most common conditions for controllers to rely on are that:

- the data subject consents to the processing
- the processing is necessary for the performance of a contract to which the data subject is a party or between a controller and a third party in the interests of a data subject, or is in order to take steps at the data subject's request with a view to entering into a contract
- the processing is necessary for the controller to exercise any right or power, or perform or comply with a duty imposed on it by law, otherwise than an obligation imposed by an enactment, an order, or a judgment of a court or tribunal having the force of the law in the Bailiwick
- the processing is necessary in order to protect the vital interests of the data subject
- the processing is necessary for legitimate interests of the controller or third party except where the processing is exercised by a public authority
- the processing is necessary for the exercise or performance by a public authority of a function that is of a public nature or a task carried out in the public interest.

It is interesting to note that processing in the public interest is only available to public authorities whereas the equivalent provision in the GDPR is much broader than this.

In addition to these conditions, controllers may also rely on one or more of a restrictive set of conditions in order legitimise either personal data or special category data. These include (but are not limited to):

- the data subject providing *explicit* consent to the processing
- processing which is necessary for compliance with a legal right or power or duty imposed on a controller by an enactment
- processing which is made public as a result of steps deliberately taken by the data subject
- processing which is necessary for the purpose of or in connection with legal proceedings, the discharge of any functions of a court or tribunal, obtaining legal advice or establishing, exercising or defending legal rights

- processing which is for the administration of justice of the exercise of any function of the Crown, the States of Guernsey or a public committee
- processing which is necessary for a historical or scientific purpose
- processing is necessary for the vital interests of a data subject.

Additional bases

In addition to the above, further secondary legislation has been adopted which sets out a number of additional lawful bases which are intended to be applied in limited circumstances.

These bases include (but are not limited to):

- the processing of health or criminal data for insurance business purposes
- special category data which is required in order to perform or comply with a duty conferred by law on a controller in connection with employment
- special category data for the prevention, detection or investigation of an unlawful act.

The additional bases will need to be considered on a case-by-case basis and may not always be straightforward to apply. If there were concerns regarding the legitimacy of such processing, we would recommend that you seek Guernsey law advice.

Consent

For the purposes of Section 10 DPL 2017, where a controller seeks to rely on consent, the controller must comply with more stringent requirements than under the DPL 2001 in order to ensure that such consent is valid.

'Valid' consent involves (amongst other characteristics) a "*specific, informed and unambiguous indication of the data subject's wishes by which a data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data*". In this regard, the DPL 2017 sets the same high standards for consent as the GDPR.

Furthermore, the ODPA guidance confirms that, in addition to the ingredients required to achieve valid consent, explicit consent must be expressly confirmed in words, rather than a positive action. These requirements are summarised in a checklist for controllers setting out what controllers need to do when relying on consent.

Finally in relation to consent, Section 10(2)(f) DPL 2017 stipulates that a child may only provide their own consent to processing in respect of the information society (primarily, online) services, where that child is over 13 years of age. Otherwise, a parent (or other responsible adult) must give it on their behalf.

Transparency

Requirements of transparency under the DPL 2017 closely align with the GDPR. Therefore, the DPL 2017 requires that certain specified information must be supplied as part of a 'fair processing notice' (Schedule 3 DPL 2017), namely:

- the identity and contact details of the controller, and (where applicable), the controller's representative
- the contact details of the data protection officer (if any)
- confirmation of whether any of the personal data is special category data
- where the personal data is not obtained directly from the data subject: confirmation of the source of the personal data and (if applicable) confirmation of whether the personal data was obtained from a publicly available source and, if so, confirmation of that source
- the purposes for which the data is intended to be processed and the legal basis for the processing
- an explanation of the legitimate interests pursued by the controller or by a third party, if the processing is based on those interests
- the recipients or categories of recipients of the personal data (if any)
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and whether or not there is an adequate level of protection for the rights and freedoms of data subjects
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

- information concerning the rights of data subjects
- where the processing is based on consent, the existence of the right to withdraw consent
- a statement of the right to complain to the Authority
- the existence of any automated decision-making, meaningful information about the logic involved in such decision-making and the significance of any such decision making for the data subject
- any further information that is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable the processing in respect of the data subject to be fair.

Rights of the data subject

The DPL 2017 has strengthened the rights of data subjects in line with the GDPR (Part III DPL 2017).

Controllers must respond to a request "*as soon as practicable*" and in any event within one month following:

- the day on which the controller has received the request,
- the day on which the controller receives the information necessary to confirm the identity of the requestor, or
- the day on which a fee or charge is paid to the controller.

These provisions represent a change to the position as last stated in August 2019 by the UK ICO.

The following rights are available to data subjects:

- *Right to information for personal data collected about the data subject either directly or indirectly (Sections 12-13DPL 2017)*: Where personal data has been collected from a source other than the data subject, certain exceptions are available

- *Right to data portability (Section 14 DPL 2017)*: a data subject has the right to have certain relevant personal data (being personal data relating to that person which has been provided to the original controller directly or via a processor) ported to a new controller, where:

    - that relevant personal data is being processed based on consent; or
    - processing necessary for the conclusion or performance of a contract.

  Where the right applies, the original controller must ensure that any personal data transmitted is provided in a structured, commonly used and machine-readable format. The right is subject to certain exceptions set out under Section 16 DPL 2017

- *Right of access (Section 15 DPL 2017)*: a data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about how the data has been used by the controller. Section 16 DPL 2017 provides for certain exceptions, including where a request cannot be complied with without disclosing information about another individual[1], balancing the rights of the requestor with significant interests of the other individual. The DPL 2017 sets out further detail in respect of the factors which should be taken into consideration when making this determination.

- *Right to object to processing (Section 17 – 19 DPL 2017)*: data subjects have the right to object to processing for: (a) direct marketing purposes, (b) on public interest grounds, and (c) where the processing is for historical or scientific purposes

  Whilst the right to object in respect of paragraph (a) is unconditional, the rights to object under paragraphs (b) and (c) are qualified and subject to a public interest test

- *Right to rectification (Section 20 DPL 2017)*: a data subject has a right to request that any inaccurate or incomplete personal data may be corrected or that a statement is provided on the controller's file noting that the data subject disputes the accuracy or completeness of the personal data

- *Right to erasure (Section 21 DPL 2017)*: data subjects may request erasure of their personal data. The right is not absolute; it only arises in a relatively narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or following the successful exercise by the data

subject of their right to object or if the data subject withdraws their consent

- *Right to restriction of processing (Section 22 DPL 2017)*: a data subject may request that the processing of their personal data is restricted in certain limited circumstances. Examples include: where the accuracy of the personal data is contested; where the processing is unlawful; or, where the data is no longer required (save for legal claims or for the purposes of obtaining legal advice or establishing / exercising or defending legal rights)

- *Right to notified of restriction, erasure or rectification (Section 23 DPL 2017)*: the controller must not only notify the data subject concerned but, unless it is impracticable or involves disproportionate effort, notify any other person whose personal data has been disclosed

- *Right not to be subject to decisions based on automated processing (Section 24 DPL 2017)*: a data subject has a right not to be subjected to a decision reached through an automated process, and a controller is prohibited from causing or permitting a data subject to be subjected to an automatic decision unless Section 24(2) DPL applies.

  Section 24(2) permits automated processing where: the data subject has given their explicit consent, or the processing has been authorised by the States of Guernsey or via an enactment; or, the automated processing is necessary for the vital interests of the data subject or another person or for the performance of a contract.

  Additional restrictions apply for the automated processing of special category data. A controller must ensure that appropriate safeguards are in place where automated processing has been conducted in accordance with Section 24(2) DPL (including allowing the data subject to appeal or seek a review of the decision)

- *Right to make a complaint to ODPA (Section 67 DPL 2017)*: a data subject may also complain in writing to the ODPA if they consider that a controller or processor has breached or is likely to breach the DPL 2017 and that breach involves or affects (or is likely to involve or affect) personal data relating to the individual or any data subject right of the individual; and

- *Right to bring a civil action against a controller or processor for breach duty (Section 79 DPL 2017)*: where a controller or processor breaches an operative provision under the DPL 2017 that causes damage to another person, the injured party may bring a claim in tort against the controller or processor for breach of statutory duty. The court may award damages, impose an injunction to restrain an actual or anticipated breach of duty and / or make a declaration that the controller or processor has committed or will commit a breach if its current course of action subsists. Individuals may also claim compensation for distress, inconvenience or other adverse effect suffered by an injured party even if it does not result from any physical or financial loss or damage. Group (or 'class') actions may also be brought against an organisation (Section 97 DPL 2017).

---

1. It is worth flagging that the DPL 2017 refers to individuals as opposed to the wider concept of 'others', as the equivalent measure is set out in the GDPR. Therefore, it is unclear whether recital 63 of the GDPR would apply in a Guernsey context where the disclosure of information might adversely affect the rights and freedoms of a person other than an individual (e.g. where the disclosure of such information might prejudice the intellectual property rights of a company or partnership).

TRANSFER

The DPL 2017 differentiates between *authorised jurisdictions* and *unauthorised jurisdictions*.

Authorised jurisdictions include:

- the Bailiwick of Guernsey
- a member state of the European Union
- any country, sector or international organisation which has been determined by the European Commission as providing an 'adequate level of protection' for the rights and freedoms of data subjects or

- any *designated jurisdiction*.

A *designated jurisdiction* includes the UK (or any country within the UK), any Crown Dependency (such as the Channel Islands or Isle of Man) or any sector within the UK or a Crown Dependency.

Unauthorised jurisdictions means any countries, sectors in a country or international organisation that does not fall within the scope of an 'authorised jurisdiction'.

Personal data must not be transferred outside of the Bailiwick of Guernsey by a controller or processor ("**Exporter**") to an unauthorised jurisdiction unless the Exporter is satisfied that:

- particular 'safeguards' are in place and there is a mechanism for data subjects to enforce their rights and obtain effective legal remedies against a controller or processor receiving the personal data ("**Importer**") (section 56 DPL 2017)
- the Authority or the ODPA has authorised the transfer (section 57 DPL 2017) or
- other specified *derogations exist* (section 59 DPL 2017)

'*Safeguards*' for the purposes of paragraph (a) above include: legally enforceable agreements (where the Importer is a public authority / body), binding corporate rules, EU's Model Clauses (or equivalent provisions as may from time to time be in force) or approved codes or other approved mechanisms which combine binding and enforceable commitments on the Importer.

'*Derogations*' include:

- the data subject has given explicit consent to the transfer after having been informed of the risks of the transfer
- the transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and third party in the interests of the data subject or for the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller
- the transfer is authorised by regulations made for reasons of public interest
- the transfer is necessary for, or in connection with, legal proceedings, obtaining legal advice or for the purposes of establishing, exercising or defending legal rights
- the transfer is necessary to protect the vital interests of the data subject or another individual (provided that the data subject is physically or legally incapable of giving consent or the controller cannot be reasonably expected to obtain explicit consent)
- the transfer is part of personal data on a public register or a register to which a member of the public has lawful access
- a decision of a public authority (within or without the Bailiwick) based on international agreement imposing international obligations on the Bailiwick or an order of a court or tribunal
- the transfer is in the legitimate interests of the controller which outweighs the significant interests of the data subject and:
    - the transfer is not repetitive
    - the transfer only concerns a limited number of data subjects
    - the controller has assessed all circumstances surrounding the data transfer and on the basis of that assessment considers that appropriate safeguards to protect personal data have been provided.

Where the transfer is justified on the legitimate interests grounds described above, both the ODPA and the data subject must be notified accordingly.

Guernsey

In common with the GDPR, The DPL 2017 places restrictions on the extent to which personal data may be transferred to recipients outside the Bailiwick of Guernsey ("**Guernsey**").

As set out above, in the absence of an adequacy decision by the EC, transfers are permitted outside the EU/EEA under certain other specified circumstances, in particular where such transfers take place subject to "appropriate safeguards". The Law replicates this regime for transfers outside Guernsey.

Appropriate safeguards for such transfers include:

- Binding corporate rules ("**BCRs**").
- Standard data protection contractual clauses adopted by the European Commission ("**SCCs**").

SCCs are generally the most commonly utilised mechanism for such transfers.

In June 2021, the EC approved a new set of SCCs for international data transfers.[1]

The Guernsey data protection regulator, the ODPA, has now approved the new SCCs for international transfer as a valid transfer mechanism for data transfers from Guernsey (The European Commission's new Standard Contractual Clauses - technical update ODPA).

The new SCCs for international transfers reflect the changes made to European data protection law made by the GDPR and address some of the issues with the existing sets of SCCs (which include two controller to controller ("**C2C**") sets (2001 and 2004) and a controller to processor ("**C2P**") set (2010). The new SCCs (unlike the existing ones which only applied to C2C and C2P transfers), apply to a broader range of scenarios and include provisions for processor-to-processor ("**P2P**") and processor-to-controller ("**P2C**").

The new SCCs effectively combine all four sets of clauses into one document, allowing controllers and processors to "build" the relevant agreement on a modular basis.

The new SCCs also incorporate provisions to address the Schrems II decision of the European Court of Justice, the key effect of which was to invalidate the EU-U.S. Privacy Shield and to place additional administrative conditions on the use of SCCs.

While a transition period allows businesses to incorporate the old SCCs into new contracts until, at the latest, **27 September 2021**, any Guernsey business looking to export personal data relying on SCCs will after that date need to use the new SCCs which provide for these further steps are taken. All existing contracts must be transitioned to the new SCCs by **27 December 2022**.

Where controllers and processors are utilising SCCs (either new or old) or BCRs, they will need also to take account of the Schrems II decision. The European Data Protection Board ("**EDPB**") has published its Schrems II guidance in relation to supplementary measures to accompany international transfer tools. In summary, a 6 step process is required in relation to international transfers.

1. **Know your transfers.** Be aware of where the personal data so you know the level of protection provided there. Make sure the data you transfer is adequate, relevant and limited to what is.
2. **Verify the transfer tool your transfer relies on**. Using the SCCs or BCRs will be enough in this regard.
3. **Assess** if there is anything in the law and/or practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer.
4. **Identify and adopt supplementary measures** necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary if your assessment has revealed issues with the third party country's safeguards. If no supplementary measure is suitable, you must avoid, suspend or terminate the transfer.
5. **Take any formal procedural steps** the adoption of your supplementary measure may require.
6. **Re-evaluate at appropriate intervals** the level of protection afforded to the personal data you transfer to third countries and monitor if there have been or there will be any developments that may affect it. This is an ongoing duty.

In practice, the above requires a detailed and documented **transfer impact assessment** ("**TIA**"). For many Guernsey controllers and processors, this will be an onerous process and we would suggest that it should be something that Guernsey businesses should prioritise. We are able to assist clients in this process.

Part of the UK Information Commission consultation on international transfer referenced below includes a TIA toolkit and we would suggest that this provides an excellent and practical starting point for Guernsey controllers and processors

What about the UK?

The European Commission has recognised the UK as an adequate jurisdiction for the purposes of international data transfer,

meaning that transfers to and from the UK and Guernsey may continue without restriction.

Guernsey controllers and processors who are subject to the UK GDPR by virtue of its extra territoriality provisions will also need to consider whether they may need to continue using the existing SCCs – the UK is yet to make a decision on replacing them for the purposes of the UK GDPR.

The UK Information Commission has now published a consultation draft of its SCC alternative -– what it describes as an International Data Transfer Agreement ("**IDTA**").

The IDTA looks very different in style to the SCCs and time will tell whether those differences lead to issues between the EU and the UK.

However, it is encouraging to note that the UK's Commission has indicated that for those organisations wishing to use the European Commission approved SCCs, they will be able to do so by completing a straightforward UK addendum.

As noted above, a TIA toolkit is also included.

---

[1] It should be noted that the European Commission also approved a set of SCCs in relation to data processing agreements at the same time.

SECURITY

Security features more prominently under the DPL 2017 than its predecessor. Whilst implementing appropriate security measures to safeguard personal data from unauthorised or unlawful processing continues to be a feature of the DPL 2017 (see Principle 6 'Integrity and Confidentiality'), the DPL 2017 (unlike its predecessor) sets out with more clarity the steps required to ensure compliance.

Data controllers must take reasonable steps to ensure a level of security which is appropriate to the personal data, taking into account the nature, scope, context and purpose of the processing, the likelihood and severity of the risks to data subjects if the personal data is not secure (including the risk of unlawful or accidental destruction, loss or alteration and / or unauthorised disclosure of personal data), best practice and the costs of implementing appropriate measures.

Section 41 of the DPL 2017 provides some assistance as to what may be regarded as a reasonable 'step' to ensure appropriate security. In essence, to ensure compliance with this obligation, a controller should consider:

- pseudonymising and encrypting personal data
- ensuring that the controller or processor has and retains the ability to:
    - ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
    - restore access to personal data in a timely manner in the event of a physical or technical incident; and
- establishing and implementing a process for regular testing and evaluation of the effectiveness of the technical and organisational measures.

There are several provisions which touch on the security obligations, located throughout the DPL 2017. Thus, the key provisions not only appear in the main security section (Part VI of the DPL 2017) but also form a key consideration (amongst other things) when undertaking a data protection impact assessment, the right to erasure, a controller's duty to take reasonable steps to achieve compliance and the measures that should be in place when choosing a processor. For example, when assessing the suitability of a processor a controller must ensure that the processor provides sufficient guarantees that reasonable technical and organisational security measures governing the processing will be established to meet the requirements of the DPL 2017.

BREACH NOTIFICATION

What is a breach?

The DPL 2017 defines a 'personal data breach' as a "*breach of security leading to the (a) accidental or unlawful destruction, loss, or*

alteration of; or, (b) unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

This definition replicates the definition set out in Article 4 of the GDPR.

Notice to ODPA

As with the GDPR, the DPL 2017 requires all controllers, upon becoming aware of a personal data breach to provide written notice to the ODPA as soon as practicable and no later than **72 hours** after becoming so aware. Section 42(5) of the DPL 2017 provides an exemption from the duty to notify the ODPA where the personal data breach is "*unlikely to result in any risk to the significant interests of the data subject*".

In determining whether or not there is a risk, the ODPA's guidance entitled '*Notification of Personal Data Breaches*' ("**Breach Guidance**") advises organisations who process personal data to consider the type of personal data they hold and whether any breach could, both at the time of the breach and in the future, 'adversely affect an individual' taking into consideration the potential for financial loss, reputational damage, or identity fraud.

The DPL 2017 stipulates the sort of information which must be provided to the ODPA in the event of such a breach including a description of the nature of the personal data breach, contact details of the DPO or contact point, a description of the likely consequences of the breach, a description of the measures taken or proposed to be taken to address risks and mitigate against possible adverse effects and an explanation of any delays (where a breach has been notified after 72 hours).

All breaches which must be notified to the ODPA can be submitted to the ODPA via their online secure breach reporting facility.

In any case, whether a personal data breach is notified to the ODPA or not, the controller must keep a written record of each personal data breach of which the controller is aware, including the facts relating to the breach, the effects, the remedial action taken and any steps taken by the controller to comply with its notification obligations (including a copy of the notice provided to the ODPA).

Notice to data subjects

Where a controller becomes aware of a personal data breach that is likely to pose a "*high risk to the significant interests of a data subject*", the controller must give the data subject written notice of the breach as soon as possible.

The Breach Guidance provides a non-exhaustive of factors for controllers to take into account when determining whether a breach poses a 'high risk'. Whilst financial loss, reputational damage and identity fraud must be considered, the Breach Guidance also includes the risk of whether the breach might have an adverse impact of safety or wellbeing of the data subject (including psychological distress or humiliation). When assessing the risks, the ODPA expects all controllers to consider the nature, scope, context and purpose of the compromised personal data, including whether special category data had been compromised.

Any notice given to an affected data subject must include a description of the nature of the breach, the name and contact details of the DPO or point of contact, a description of the likely consequences of the breach, and a description of the measures taken or proposed to be taken by the controller to address the breach.

A controller is exempt from the requirement to notify a data subject where it has:

- established and carried out appropriate technical and organisational measures to protect personal data and, in particular, those measures have rendered personal data unintelligible to any person who is not authorised to access it (e.g. encryption); or
- taken subsequent measures to mitigate the risk, such that the 'high risk' is no longer likely to materialise, or where the performance of the duty would involve 'disproportionate effort'.

Whilst the Breach Guidance does not define what will amount to 'disproportionate effort to notify', it clarifies that a controller must nonetheless publish a notice (without making public any personal data) or take any other step equivalent to publication in order to inform the data subjects in an equally effective manner.

Notice to controller (where a processor is engaged)

The responsibility for reporting a personal data breach to the ODPA rests with the controller. However, where a processor becomes aware of a personal data breach, the processor must give the controller notice as soon as practicable. Where notice is given orally, written notice must follow at the first available opportunity.

Other regulatory notification requirements

Guernsey's European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance 2004 (as amended) ("**e-Privacy Ordinance**") requires a provider of a public electronic communications service (the '**service provider**') to notify subscribers of a significant risk to the security of the service.

ENFORCEMENT

The Authority and the ODPA are responsible for administering and enforcing the DPL 2017 (Section 61(1)(a) DPL 2017).

When investigating a complaint regarding a potential breach of the DPL 2017, the Authority has wide powers to require information and, with appropriate warrants, powers to enter premises and search them (Schedule 7 DPL 2017). It may also conduct and / or require an audit of a controller or processor.

Before making a breach determination or an enforcement order, the ODPA may give the person concerned a written notice of the ODPA's proposals and allow the person time (up to 28 days) to make representations. However, the ODPA may dispense with this requirement if the determination or order needs to be made immediately or without notice in the interests of the data subjects or where the ODPA has reasonable grounds for suspecting that data may be tampered with or that to do so might seriously prejudice any other investigation etc. There is a right to appeal the decision of the ODPA under section 84 DPL 2017.

Following a breach determination, the ODPA may take the following enforcement action:

Reprimand

The DPL 2017 does not specify the conditions upon which a reprimand may be issued. However, it will most likely take the form of a notice issued in combination with an administrative fine or a formal undertaking by the controller or processor to meet future compliance with any part of the DPL 2018.

Warning

A warning may be given where the ODPA determines that any proposed processing or other act or omission is likely to be a breach of the DPL.

Order

This refers to a formal notice of enforcement and can consist of an order to do any or all of the following:

- bring specified processing operations into compliance with an operative provision of the DPL 2017, or take any other specified action required to comply with said provision, in a manner and within a period specified in the order
- notify a data subject of any personal data breach
- comply with a request made by the data subject to exercise a data subject right
- rectify or erase personal data
- restrict or limit the recipient's processing operations (which may include restricting or ceasing the processing operation or suspending any transfers to an unauthorised jurisdiction)
- notify persons to whom the personal data has been disclosed of the rectification, erasure or temporary restriction on processing

Administrative fines

Whilst the GDPR has the potential to attract administrative fines of up to 4% of annual worldwide turnover or EUR 20 million (whichever is higher), the administrative fines under the DPL 2017 are generally lower (between £5,000,000 - £10,000,000) and

can be broadly categorised on four levels.

Level 1

Administrative fines issued against a controller or processor may not exceed £5,000,000 for breaches of section 74(1)(a) – (d) DPL 2017, comprising the following:

- failure to make reasonable efforts to verify that a person who has given consent to the processing of a child's personal data (being a child who is under 13 years' old) in the context of offering information society services directly to that child, is duly authorised to give consent to that processing under Section 10(2)(f) DPL 2017
- failure to take reasonable steps to inform the data subject of anonymisation (in breach of Section 11(1)(b) DPL 2017)
- any breach of the general duties of controllers and processors (except section 31 DPL 2017 – duty to take reasonable steps for compliance) (breach of Part IV DPL 2017)
- any breach of a controller's administrative duties including the requirement to designate a representative in the Bailiwick in certain cases and the requirement to register and pay fees to the ODPA (as per Part V DPL 2017)
- a breach of the security provisions contained in Part VI DPL 2017
- failure to comply with the requirements in respect of data protection impact assessments and prior consultation (except section 46 DPL 2017 – prior consultation required for high-risk legislation) in accordance with Part VII DPL 2017
- failure to comply with requirements to designate a DPO (where required) or ancillary duties relating to the DPO's functions in accordance with breach of Part VIII of the DPL 2017.

Level 2

Administrative fines issued against a controller or processor may not exceed £10,000,000 for breaches of section 74(1) DPL 2017, comprising the following (in addition to the Level 1 list above):

- breach of any duty imposed on the person concerned by section 6(1) (data protection principles) including lawfulness of processing
- breach of any duty imposed on the person concerned under Part III DPL 2017 (data subject rights)
- failure to comply with an order by the Authority under section 73(2) DPL 2017 within the time specified in the order
- transfer of personal data to a person in an unauthorised jurisdiction in breach of section 55 DPL 2017 (general prohibition of transfers of personal data outside of the Bailiwick to unauthorised jurisdictions)
- breach of any provision of any ordinance or regulations made pursuant to the DPL 2017 which imposes a duty on a controller or processor.

Level 3

In addition to the two administrative fines described above, the DPL 2017 imposes a 'cap' on administrative fines of up to £300,000 (unless the fine is less than 10% of the person's total annual global turnover or total global gross income in the preceding financial year).

Level 4

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

Enforcement activity has increased since the implementation of the DPL 2017 and more specifically during the last 12 months. To date, we are aware that two Guernsey controllers have been subject to administrative fine orders for the sum of £80,000 and £10,000 respectively. We are also aware that the ODPA has issued both public and private reprimands on controllers (the severity of which depends on the seriousness of the breach).

Offences / criminal proceedings

In addition to the above, the DPL 2017 imposes criminal sanctions on persons who are found guilty of certain specified offences. Such offences include:

a. unlawful obtaining or disclosure of personal data
b. obstruction or provision of false, deceptive or misleading information
c. impersonation of an Authority official, and
d. (unless an exception applies) breach of confidentiality by a designated official without the consent of the individual.

Regarding the offence under paragraph (d) above, a 'designated official' shall include a member of the Authority including the Commissioner and any DPO.

Criminal liability can attach to any director or other officer of the organisation including a body corporate, general partner of a limited partnership, foundation official etc. Criminal proceedings may also be instigated against an unincorporated entity in the case of a general partnership, or a committee etc.

ELECTRONIC MARKETING

Direct marketing by electronic means to individuals and organisations is regulated by the European Communities (Implementation of Privacy) Directive (Guernsey) Ordinance 2004 ("**e-Privacy Ordinance**").

Following the implementation of the DPL 2017, minor and consequential changes were made to the e-Privacy Ordinance, which is intended to sit alongside the DPL 2017.

In this regard, neither the e-Privacy Ordinance nor the DPL 2017 prohibit the use of personal data for the purposes of electronic marketing provided that individuals have the right to prevent the processing of their personal data (i.e. a right to 'opt out') for direct marketing purposes.

As such, the e-Privacy Ordinance still reflects the e-Privacy Directive and, for example, prohibits the use of automated calling systems without the consent of the recipient. Furthermore, unsolicited emails can only be sent without consent if:

- the contact details have been provided in the course of a sale or negotiations for a sale
- the marketing relates to a similar product or service, and
- the recipient was given a simple method of refusing the use of their contact details when they were collected.

The identity of the sender cannot be concealed in direct marketing communications sent electronically (which is likely to include SMS marketing).

These restrictions only apply in respect of individuals and not where corporations are sent marketing communications.

ONLINE PRIVACY

The 2011 amendments to the Privacy and Electronic Communications Regulations 2003 by the UK in relation to cookies did not find their way into Guernsey law and there are no immediate plans for this to be done. However, certain aspects of online privacy nevertheless remain governed by the e-Privacy Ordinance (defined under Electronic Marketing above).

As a matter of good practice:

- the use of cookies should be identified to web users
- cookies should be accompanied with a description of what the cookies are doing and why they are being used
- consent should be obtained (at least initially) from the web user where the website intends to store a cookie on their device.

Consent in this context must be freely given, specific, informed and an unambiguous positive action (although it does not need to be explicit).

Traffic data held by a service provider must be erased or anonymised when it is no longer necessary for the purpose of a transmission or communication and only used for permitted purposes. It must also be accompanied by information as to the nature of the processing. Exceptions include if the information is being retained in order to provide a value added service to the data subject or if it is held with their consent.

Traffic data should only be processed by a service provider for (a) the management of billing or traffic, (b) customer enquiries, (c) the prevention or detection of fraud, (d) the marketing of electronic communications services, or (e) the provision of a value added service.

Location data may only be processed in circumstances where the organisation processing such data is a public communications provider, a provider of a value added service, or a person acting on the authority of such provider and only where the user / subscriber cannot be identified from that data (i.e. because they are anonymous) or for the provision of a value added service with consent.

Given the fundamental changes to the data protection regime since the e-Privacy Ordinance was introduced in 2004 and the ongoing negotiations in Europe in relation to the so-called 'e-Privacy Regulation' ("**Regulation**"), further amendments to the e-Privacy Ordinance are, perhaps, inevitable. The States of Guernsey continues to monitor the progress of the draft Regulation in the meantime.

KEY CONTACTS

Carey Olsen (Guernsey) LLP
www.careyolsen.com

Robin Gist
Senior Associate
Carey Olsen (Guernsey) LLP
T +44 (0)1481 732095
robin.gist@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.