DATA PROTECTION LAWS OF THE WORLD

Jersey

JERSEY

Last modified 11 January 2024

LAW

The Data Protection (Jersey) Law, 2018 (DPJL) and the Data Protection Authority (Jersey) Law, 2018 (DPAJL) came into force on May 25, 2018. These laws superseded the Data Protection (Jersey) Law 2005, which had been held to be adequate by the European Commission for the purposes of the European Data Protection Directive (Directive 95/46/EC) (see Commission Decision 2008/393/EC). This decision continues to apply pending a review of Jersey's adequacy (to be conducted under Article 45 of the European General Data Protection Regulation (GDPR)), the outcome of which was expected in 2021 but is now expected during 2023.

The DPJL and DPAJL provide a broadly equivalent regime to that under the GDPR.

DEFINITIONS

The DPJL defines 'data' as information that:

- Is processed by means of equipment operating automatically in response to instructions given for that purpose or is recorded with the intention that it should be processed by means of such equipment
- Is recorded as part of a filing system or with the intention that it should form part of a filing system, or
- Is recorded information held by certain public authorities

The DPJL defines 'personal data' as being any data relating to a data subject.

A 'data subject' is defined in the DPJL as an identified or identifiable, natural living person who can be identified, directly or indirectly, by reference to (but not limited to) an identifier such as:

- A name, an identification number or location data
- An online identifier (which may include an IP address, location data or any unique number or code issued to the individual by a public authority), or
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person

Enhanced levels of protection in the DPJL and DPAJL are provided for 'special category' personal data.

'Special category personal data' is defined under the DPJL as personal :

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership
- Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person’s sex life or sexual orientation, or
- Data relating to a natural person’s criminal record or alleged criminal activity

Personal data may be processed by either a '**controller**' or a '**processor**'. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 1(1) DPJL). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the DPJL imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

NATIONAL DATA PROTECTION AUTHORITY

The DPAJL created a Data Protection Authority (the Authority) to oversee the DPJL. Save in respect of certain matters (in particular the issuing of a formal public statement in relation to data protection issues or the issuing of an administrative fine), its functions are delegated to the Information Commissioner.

REGISTRATION

Registration and fees are governed by the Data Protection (Registration and Charges) (Jersey) Regulations 2018 (as amended) (the "**Regulations**") under which annual processing fees are charged, the value of which are based on:

- the number of full-time employees;
- the level of past-year revenue;
- whether the relevant entity is a regulated financial services provider (or otherwise subject to the Money Laundering (Jersey) Order 2008);
- if the entity processes special category data; and
- if the entity is administered by a trust company business or fund services business, and if so, the name of the administrator.

The maximum fee payable on the basis of the above is £1,600. However, the majority of data controllers and processors pay £70.

Entities that are administered by a regulated trust company business or fund services business are required to pay a fixed annual charge of £50. No fees are payable where the entity does not process data (as they would not be considered data controllers or processors).

All controllers and processors are required to renew their registration annually. It should be noted that, external accountability to the Information Commissioner via registration or notification has in many ways superseded in the DPAJL and DPJL by rigorous demands for internal accountability.

In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 14(3) DPJL), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request.

DATA PROTECTION OFFICERS

Data controllers and processors are required (Article 24 DPJL) to appoint a data protection officer if:

- Processing is carried out by a public authority (with the exception of courts acting in their judicial capacity)
- The core activities of the controller or the processor consist of processing operations that, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller or the processor consist of processing special category data on a large scale, or
- It is otherwise required by law

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 24(3) DPJL). However, larger corporate groups may find it difficult in practice to operate with a single data protection officer. The data protection officer must be easily accessible to:

- All data subjects
- The Information Commissioner, and

- The controller or processor who appointed the officer, along with the controller’s or processor’s employees that carry out data processing

Data protection officers (DPOs) must have expert knowledge (Article 24(6) DPJL) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 24(7) DPJL).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 25(1) DPJL), and the DPO must directly report to the highest management level of the controller or processor (Article 25(2) DPJL).

In addition, controllers and processers must:

- Ensure that the data protection officer operates independently and does not receive any instructions regarding the performance of those duties, other than to perform them to the best of the officer’s ability and in a professional and competent manner (Article 25(1)(c) DPJL), and
- Not dismiss or penalize the data protection officer for performing his or her duties other than for failing to perform them to the best of the officer's ability and in a professional and competent manner (Article 25(1)(d) DPJL)

The specific tasks of the DPO are set out in Article 26 DPJL and include:

- Informing and advising on compliance with the DPJL, DPAJL and other applicable data protection laws
- Monitoring compliance with the law and with the internal policies of the organization, including assigning responsibilities, raising awareness and training staff
- Advising on and monitoring data protection impact assessments, where requested, and
- Cooperating and acting as point of contact with the Information Commissioner

COLLECTION & PROCESSING

Controllers are responsible for compliance with a set of core principles that apply to all processing of personal data. Under these principles, personal data must be (Article 8(1) DPJL):

- Processed lawfully, fairly and in a transparent manner in relation to the data (‘lawfulness, fairness and transparency’)
- Collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes (‘purpose limitation’)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’)
- Accurate and, where necessary, kept up-to-date, with reasonable steps being 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 (‘accuracy’)
- 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 (‘storage limitation’) and
- Processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’)

Additionally, the controller is responsible for and must be able to demonstrate compliance with the above principles (‘accountability’) (Article 6(1)(a) DPJL).

Accountability is a core theme of the DPJL. Organizations must not only comply with the DPJL, but also be able to *demonstrate* compliance, perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving (and being able to demonstrate) accountability.

Legal Basis for Processing

The DPJL works slightly differently to the GDPR in terms of establishing a legal basis for processing.

Data controllers may collect and process personal data when any of a number of conditions are met (Article 9 and Schedule 2 DPJL). The most frequently relied upon are as follows:

- The consent of the data subject
- The processing is necessary for:
  - The performance of a contract to which the data subject is a party, or
  - The taking of steps at the request of the data subject with a view to entering into a contract
- The processing is necessary to comply with a data controller’s legal obligations (other than one imposed by contract)
- The processing is necessary to protect the data controller’s vital interests
- The processing is necessary for:
  - The administration of justice
  - The exercise of any functions conferred on any person by or under any enactment
  - The processing is necessary for taking legal advice or the establishment, exercise or defense of legal claims
  - The exercise of any functions of the Crown, the States or any public authority, or
  - The exercise of any other functions of a public nature with a legal basis in Jersey law to which the controller is subject and exercised in the public interest by any person
  - The processing is necessary for the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, unless:
    - The processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject, in particular where the subject is a child, or
    - The controller is a public authority, or
  - The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject

Special Categories of Data

Where special category personal data is processed, at least one of a more restrictive list of conditions than those for personal data must be satisfied (Article 9 and Schedule 2 Part 2 DPJL). Unlike the GDPR, personal data may also be processed on the basis of the conditions for processing special category data. The most frequently relied upon bases for processing special category data are as follows:

- The explicit consent of the data subject
- The processing is necessary to comply with a data controller’s legal obligations (other than one imposed by contract)
- The processing is necessary for the purposes of exercising or performing any right, obligation or public function conferred or imposed by law on the controller in connection with employment, social security, social services or social care
- The processing is necessary for taking legal advice or the establishment, exercise or defense of legal claims
- The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- The processing relates to personal data which are manifestly made public by the data subject
- The processing is necessary for archiving or research
- The processing is necessary for the prevention of unlawful acts (or malpractice / mismanagement)
- The processing is necessary for certain insurance-based purposes, or
- The processing is necessary for medical purposes and is undertaken by a health professional

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data *(ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected). This is potentially in conflict with the core principle of

purpose limitation, which aims to ensure that the rights of data subjects are protected. The DPJL sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 13 DPJL)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are, it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects, and
- The existence of appropriate safeguards

Transparency

The data controller must provide the data subject with “fair processing information” (Article 12 DPJL), which includes:

- 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)
- The purposes for which the data are 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 organization and whether or not there is an adequate level of protection for the rights and freedoms of data subjects in that country or organization
- 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
- The existence of any automated decision-making and any meaningful information about the logic involved in such decision-making and the significance of any such decision-making for the data subject
- A statement of the right to complain to the Information Commissioner
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failing to provide such data
- Where the personal data are not obtained directly from the data subject, information identifying the source of the data
- Any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in limited circumstances. Controllers must provide information on action taken in response to requests within four weeks as a default, with a limited right for the controller to extend this period a further eight weeks where the request is onerous. These periods are slightly shorter than those set out in the GDPR.

Right of access (Article 28 DPJL)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 31 DPJL)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 32 DPJL)

Data subjects may request erasure of their personal data.

The right is not absolute; it only arises in a 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 as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 33 DPJL)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed other than for legal claims of the data subject or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 34 DPJL)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format.

Right to object (Article 21 DPJL)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is for a public function. Controllers will then have to suspend processing of the data until such time as they demonstrate ‘compelling legitimate grounds’ for processing that override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time (Article 36 DPJL).

The right not to be subject to automated decision taking, including profiling (Article 38 DPJL)

Automated decision-making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. Necessary for entering into or performing a contract
2. Authorized by Jersey law or by the law of another jurisdiction in the British Isles or by EU or member state law, or
3. The data subject has given their explicit consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the controller must implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, including the right to obtain human intervention on the part of the controller, so that the data subject can express his or her point of view and contest the decision.

Children’s consent to information society services (Article 11(4))

Article 11(4) of the DPJL stipulates that a child may only provide his or her own consent to processing in respect of information society (primarily, online) services, where that child is over 13 years of age. Otherwise, a parent (or other responsible adult) must provide consent on the child’s behalf.

Processing agreements

The rules on agreements (or other legally binding instruments) between controllers and processors have been significantly enhanced.

The controller must appoint the processor in the form of a **binding written agreement** that sets out:

- The **subject matter** and **duration** of the processing
- The **nature** and **purpose** of the processing
- The **type of personal data** and **categories of data subjects**, and
- The obligations and rights of the controller

The agreement must also provide that the processor must:

- Only act on the controller's **documented** instructions (unless legally obliged to do otherwise)
- Impose **confidentiality obligations** on all **personnel** who process the relevant data
- Ensure the **security** of the personal data that it processes
- Abide by the rules regarding appointment of **sub-processors**
- Implement measures to assist the controller in complying with the rights of data subjects
- Assist the controller in:
    - Complying with its **data security obligations**
    - Complying with its **personal data breach** obligations (both to a supervisory authority and individual data subjects), and
    - Completing **Data Protection Impact Assessments** and **obtaining approvals from Supervisory Authorities** where required
- At the controller's election, either **return or destroy the personal data** at the end of the relationship (except as required by law), and
- Provide the controller with **all information necessary** to demonstrate compliance with the DPJL, which, in practice, means complying with an audit/inspection regime

TRANSFER

The DPJL (Article 67) provides that data controllers and processors may only transfer personal data out of the European Economic Area if one of the following conditions are met:

- The transfer is to a jurisdiction which has been held by the European Commission to provide an adequate level of protection for personal data.
- The transfer is made subject to ‘appropriate safeguards’ (Article 68 DPJL), which may include:
    - A legally binding and enforceable instrument between public authorities
    - Binding corporate rules approved by Jersey's Information Commissioner or another competent supervisory authority under the GDPR (or equivalent statutory provisions), or
    - Standard data protection clauses adopted by the Authority or by a competent supervisory authority and approved by the European Commission. It should be noted that the EDPB approved a new set of standard contractual clauses in June 2021, which have now been approved for use in Jersey (subject to also using a Jersey law addendum). It should be noted that the UK International Data Transfer Agreement has not yet been approved for use in Jersey.
- An exemption applies, the most commonly utilized of which are as follows:
    - The transfer is specifically required by a Jersey court
    - The data subject explicitly consents
    - The transfer is necessary for the performance of a contract to which the data subject is party or the implementation of pre-contractual measures taken at the data subject’s request
    - The transfer is necessary to carry out a contract between the data controller and a third party if the contract serves the data subject’s interests
    - The transfer:
        - Is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)
        - Is necessary for the purpose of obtaining legal advice, or
        - Is otherwise necessary for the purposes of establishing, exercising or defending legal rights
    - The transfer protects the data subject’s vital interests where:
        - The data subject is physically or legally incapable of giving consent

- The data subject has unreasonably withheld consent, or
- The controller or processor cannot reasonably be expected to obtain the explicit consent of the data subject

Transfers post Schrems II

The burden on Jersey controllers and processors of transferring personal data to unauthorised jurisdictions has increased following the CJEU's Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited*, Maximillian Schrems and intervening parties ("**Schrems II**").

Following Schrems II, where Standard Contractual Clauses ("SCCs") are used, controllers (and where applicable processors) must ensure that they have considered their transfers and taken any steps appropriate to ensure that they are lawful.

However, the guidance does not provide any assistance as to what steps need to be taken in order to ensure that the chosen safeguards are appropriate. The required approach has since been clarified by the European Data Protection Board which published Recommendations 01/2020 in June 2021 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (see below). There is also local Jersey guidance which broadly tracks (and cross refers to) the EDPB guidance.

The emphasis is on controllers / processors to satisfy themselves that the transfers to unauthorised jurisdictions are properly assessed (taking into account the law and practice of the recipient jurisdiction) and, as appropriate, put in place supplementary measures.

CJEU jurisprudence is not binding in Jersey, as Jersey is not an EU member state. However, it is likely to be persuasive (as is the EDPB guidance noted above).

The EDPB guidance referenced above recommends a 6 step process 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 necessary.
2. **Verify** the transfer tool your transfer relies on.
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, the exporter 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**").

Transfers between Jersey and the USA

The replacement of the Privacy Shield transfer scheme (invalidated by Schrems II) by the EU-US Privacy Data Privacy Framework means that Jersey controllers and processors are in principle able to utilise the new Framework for data transfers. However, the US Department of Commerce is yet to extend the scope of the Framework to cover Jersey and accordingly it is recommended that Jersey controllers and processors continue to utilise standard contractual clauses in respect of transfers between Jersey and the US.

What about the UK?

The European Commission has now recognised the UK as an adequate jurisdiction for the purposes of international data transfer and the UK has in turn recognised Jersey as an adequate jurisdiction for the purposes of the UK GDPR meaning that transfers to

and from the UK and Jersey may continue without restriction.

Jersey 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 standard contractual clauses or the UK International Data Transfer Agreement.

SECURITY

Controllers and processors must implement technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data that are proportionate to the risk of harm posed to the rights of data subjects by such events (Article 21 DPJL).

'Technical measures' may include:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing 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 organizational measures for ensuring the security of the processing

BREACH NOTIFICATION

The DPJL includes obligations related to ‘personal data breaches’, which are defined in the DPJL as breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data controllers must notify the Information Commissioner via an online portal (https://oicjersey.org/breach-reporting/) that a personal data breach has occurred within 72 hours of becoming aware of the breach (Article 20 DPJL). A breach does not need to be notified to the Information Commissioner where it is unlikely to result in a risk to the rights and freedoms of natural persons in respect of their personal data. If there is a high risk that the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the data controller must also notify those individuals.

Controllers are also required to keep a record of all data breaches (Article 20(5) DPJL) (whether or not notified to the Information Commissioner) and permit audits of the record by the Information Commissioner.

ENFORCEMENT

In Jersey, the Authority is responsible for the enforcement of the DPJL and DPAJL. Its day-to-day powers are delegated to the Information Commissioner, with the exception of the issuing of public statements and imposing fines.

The Authority has wide powers to require information and to enter and search premises (Schedule 1 DPAJL). It may also conduct and/or require an audit of a controller or processor.

The Information Commissioner may take the following enforcement actions:

Reprimand

The DPAJL does not specify the conditions upon which a reprimand may be issued; however most will likely take the form of a notice, and may be 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 DPJL or DPAJL.

Warning

This sanction applies where it appears to the Information Commissioner that the intended processing or other act or omission is likely to contravene the DPJL or DPAJL. Such warnings may be issued by way of a formal notice in advance of any intended

processing.

Order

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

- Bring specified processing operations into compliance with the DPAJL or DPJL, or take any other specified action required to comply with the same, in a manner and within a period specified in the order
- Notify a data subject of a 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, and
- Notify persons to whom the personal data has been disclosed of the rectification, erasure or temporary restriction on processing

Administrative Fines

The DPAJL also empowers the Authority to impose administrative fines (Article 26 DPAJL), which may be imposed in addition to any other sanctions.

An administrative fine must not exceed £300,000 or 10% of the person’s total global annual turnover or total gross income in the preceding financial year, whichever is the higher (Article 27(2) DPAJL).

An administrative fine ordered against any person whose processing of data that gave rise to the fine was in the public interest and not for profit must not exceed £10,000 (Article 27(3) DPAJL).

Subject to the above limits, an administrative fine of up to £5 million may be ordered for:

- Failure to make reasonable efforts to verify that a person giving consent to the processing of the personal data of a child as required by Article 11(4) of the DPJL (information society services) is a person duly authorized to give consent to that processing
- Breach of Article 7 of the DPJL (obligations of joint controllers)
- Breach of Part 3 of the DPJL (which includes record-keeping obligations, data protection by design and default, data protection impact assessments, appointment conditions for data processors and breach notification)
- Breach of Part 4 of the DPJL (which includes information security obligations and general obligations on processors), and
- Breach of Part 5 of the DPJL (which includes obligations relating to data protection officers)

An administrative fine of up to £10 million may be imposed for:

- Breach of Part 2 of the DPJL (which includes fundamental duties of controllers, including compliance with the data protection principles, data subject information provisions and rules regarding consent) other than for Articles 7 and 11(4), and
- Breach of Part 6 of the DPJL (Data Subject Rights)

Right to claim compensation

The DPJL makes specific provision for individuals to bring private claims against controllers and processors.

Where a controller has breached the transparency and data subject rights provisions of the DPJL, a data subject may ask the Royal Court to make such order as it considers appropriate, which may include:

- An award of compensation for loss, damage or distress in respect of the violation
- An injunction (including an interim injunction) to restrain any actual or anticipated violation
- A declaration that the controller is responsible for the violation or that a particular act, omission or course of conduct on the part of the controller would result in a violation, and
- Requiring the controller to give effect to the transparency and data subject rights provisions (unless, in the case of a data

subject access request, the Royal Court is satisfied that complying with the request will cause serious harm to a third party's physical or mental health)

Any person who has suffered "loss, damage or distress" as a result of a breach of the DPJL has the right to receive compensation (Article 69 DPJL) from the controller or processor. This means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss. In addition, data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 70). Individuals also enjoy the right to lodge a complaint with the Information Commissioner in relation to any violation of the DPJL that affects him or her (Article 19 DPAJL). Last, all natural and legal persons, including individuals, controllers and processors, have the right to complain to the Royal Court about a decision, or failure to make a decision, of the Authority or Information Commissioner concerning him or her.

Offenses

The DPJL contains the following offenses:

- Unlawfully obtaining personal data (Article 71 DPJL)
- Requiring a person to produce certain records (Article 72 DPJL)
- Providing false information (Article 73 DPJL), and
- Obstruction (Article 74 DPJL)

The DPAJL contains the following offenses:

- Failing to register with the Authority as a controller or processors (Art.17(6) DPAJL), and
- Failing to comply with an order made by the Authority following a breach determination (Article 25(8) DPAJL)

If a company or other organization commits a criminal offense under the DPJL or DPAJL, any partner, director, manager, secretary or similar officer or someone purporting to act in such capacity is personally guilty of an offense in addition to the corporate body if:

- The offense was committed with his or her consent or connivance, or
- The offense is attributable to any neglect on his or her part

ELECTRONIC MARKETING

The DPJL applies to most electronic marketing activities, as they involve some use of personal data (e.g. an email address that includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller.

Where consent is relied upon, the strict standards for consent under the DPJL apply, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the checking of an unchecked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 36 DPJL).

ONLINE PRIVACY

Jersey has no specific law regulating online privacy; however, the DPJL and DPAJL generally apply.

KEY CONTACTS

Carey Olsen Jersey LLP
www.careyolsen.com

Huw Thomas
Partner
Carey Olsen Jersey LLP
T +44 1534 888900
huw.thomas@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.