JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

JOIC REGULATORY ACTION & ENFORCEMENT POLICY

DATA PROTECTION

INTRODUCTION

The Jersey Data Protection Authority (**JDPA**) is the independent regulatory authority that promotes respect for the privacy & information rights of individuals through oversight of the Data Protection (Jersey) Law 2018 and Data Protection Authority (Jersey) Law 2018.

The main vision of the JDPA is to foster a prosperous island community that balances and embraces a collaborative and innovative approach to data protection, whilst providing a leading-edge model to other, similar jurisdictions. This vision is an essential pillar to maintaining Jersey's position as a well regulated, safe place to do business, and is of fundamental importance to Jersey's economy, recognising that alongside its traditional agricultural and tourism industries, Jersey is also a globally recognised international finance centre. In addition, maintaining the social well-being of Jersey's citizens by ensuring that individuals' privacy is regarded as a fundamental human right is core to the JDPA's focus.

The JDPA will strive to promote the data protection rights of individuals, be they our local citizens or international stakeholders, through a practical and ethical approach to business practice and regulation that supports the delivery of public services, and promotes the social and economic interests of the Island.

The above vision and promise is supported by the 3 core outcomes of the JDPA's Strategic Plan which are detailed as follows:

OUTCOME 1	OUTCOME 2	OUTCOME 3
To provide individuals with a high level of data protection and expert service, while managing resources judiciously and responsibly.	To raise the profile of data protection in Jersey, locally and internationally, in support of the island's reputation as a well-regulated jurisdiction and a safe place to store data.	To embrace innovation in assisting Jersey to become a world leader in the safe development and implementation of digital technology.

With the above in mind, an effective, fair and proportionate regulatory action and enforcement policy provides a critical framework for meeting these 3 core objectives. This document sets out how the Jersey Office of the Information Commissioner (JOIC) intends to mobilise this policy.

OVERVIEW

The JOIC's Regulatory Action and Enforcement Policy sits under the JDPA's Strategic Outcomes as detailed above and informs the organisation's 2019 – 2021 Business Plan.

Two of the JOIC's core objectives are to provide individuals with a high level of data protection and expert service, and raise the profile of data protection in Jersey in support of the Island's reputation as a well regulated jurisdiction and a safe place to store data. Achieving these objectives requires a Regulatory Action and Enforcement Policy that aims to increase levels of compliance across all industry sectors through an approach that recognises five key principles:

I. **Proportionate** - Any action taken, or intervention required by the JOIC, including monitoring, compliance or investigation, is proportionate to specific, identified risk.

II. **Targeted** - Those involved in high risk data processing activities, those carrying out activity in high risk areas such as the medical profession, those involved in novel or complex activities, and/or those with a previous history of non - compliance can expect a greater level of monitoring.

III. **Accountable** - The JOIC is accountable for the more general effectiveness of our regulatory action to Ministers. The JOIC is also accountable to the Courts for its regulatory action in specific cases. As a broader principle, the JOIC is accountable to the JDPA and the public at large;

IV. **Consistent** – The JOIC's actions are consistent, in that it should be mindful to make coherent (but not necessarily the same) decisions about action with a similar factual matrix, in accordance with its delegated responsibilities, statutory objective and guidance;

V. **Transparent** – The JOIC's approach to regulatory action is transparent by publishing information to its regulated stakeholder, indicating for example , what enforcement action it can and may take in appropriate circumstances (for example by publication of this document).

This policy provides clarity for regulated organisations, the general public and our staff as to how the JOIC will regulate the laws it is tasked with enforcing. The approach is designed to help create a safe place to store data and do business that ensures the best protection for citizens without compromising the ability of businesses to operate and innovate in the digital age. It is also designed to engender trust and build public confidence in the capacity of Jersey's public authorities to apply a high level of data protection The JOIC will take action where it is considered necessary, whilst adhering to the 5 principles above.

PART 1: THE GENERAL FRAMEWORK

Aims of the Policy

This policy seeks to:

- Set out the nature of the JOIC's various powers and be clear about how and when they will be used;
- Ensure the JOIC takes fair, proportionate and timely regulatory action in order to best protect individuals' rights;
- Guide the staff of the JOIC to ensure that regulatory action is targeted, proportionate, consistent and effective;
- Assist in the delivery of the JOIC's strategic outcomes.
- Ensure the JOIC acts in accordance with its statutory obligations under the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 (see Appendix 1).

Objectives of Regulatory Action

When considering whether to take regulatory action, and in carrying it out, the JOIC will seek to meet the following objectives:

Objective 1
To respond swiftly and effectively to breaches of the legislation that fall within the remit of the JDPA, with special attention given to: i) Those involving special category or other sensitive personal data; ii) Those adversely affecting large groups of individuals; and/or iii) Those impacting upon vulnerable individuals; iv) The source of complaints. iv) The source of complaints.

Objective 2

To be effective, proportionate, dissuasive and consistent in the application and publication of sanctions, reserving the most significant powers:

i) For organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data; and
ii) Where formal regulatory action serves as an important deterrent to those who risk non-compliance with the relevant law.

Objective 3

Promote compliance with the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018, using the promotion of good practice and provision of targeted advice on how to comply when the application of sanctions would be disproportionate.

Objective 4

To be proactive in identifying and mitigating new or emerging risks arising from technological and societal change.

Objective 5

To work with other regulators and interested parties constructively, both locally and internationally, recognising the interconnected nature of the technological landscape and data flows that exist in a growing digital economy.

The JOIC will implement these objectives by exercising our statutory powers in the following ways:

- Exercising discretion as to when, how and to what extent enforcement is required, and applying our enforcement powers in such a way that they are effective, proportionate and dissuasive;
- Taking account of, and effectively applying resources to the areas of greatest risk and potential or actual harm to individuals and the community by deciding each case on its individual merits;
- Recognising and tackling emerging threats from new technologies;
- Collaborating with the States of Jersey Police where suspected criminal offences require investigation;
- Managing risks by sharing information effectively and within the appropriate legal frameworks;
- Taking account of the application of the General Data Protection Regulation (EU) 2016/679, the UK Data Protection Act 2018 and other national or domestic data protection legislation to help achieve consistency when determining the appropriate type and level of regulatory response.

Legal basis for Regulatory Action

The JDPA has the powers (delegated to the JOIC) to take regulatory action under:

- The Data Protection (Jersey) Law 2018 – (the DPJL); and
- The Data Protection Authority (Jersey) Law 2018 – (the DPAJL).

The JOIC can also take action under:

- The Freedom of Information (Jersey) Law 2011 – (the FOIJL). This is covered under a separate enforcement policy.

PART 2: INVESTIGATIONS, ASSESSMENTS AND DETERMINATIONS

The Regulatory Action of the JOIC

The JOIC mobilises its regulatory powers (as set out in Part 4 of DPAJL) in a number of ways:

- Conducting investigations of complaints and conducting inquiries to establish compliance with the DPJL and the DPAJL;
- Issuing Information Notices;
- Making recommendations and determinations;
- Issuing orders, reprimands and warnings to Controllers and Processors following a breach of the DPJL or DPAJL;
- Issuing public statements;
- Issuing administrative fines;
- Exercising its powers of entry, search, inspection, test and seizure;
- Conducting or requiring data protection audits;
- Conducting criminal investigations where an offence under the DPJL or DPAJL has been, or is being committed, this in collaboration with the States of Jersey Police, and supporting any criminal investigation;
- Developing international cooperation mechanisms to facilitate the effective enforcement of Jersey data protection laws;
- Providing international mutual assistance in the enforcement of data protection laws;

The JOIC will be proactive in issuing guidance to controllers and processors about how to comply with the DPJL and DPAJL. Toolkits have been developed for small, medium and large businesses, and a programme of focused presentations on different aspects of the DPJL are in train. Similarly, privacy toolkits have also been developed to assist individuals in the exercise of their information rights. The full suite of guidance is available on the JOIC website and will be added to and updated regularly.

Selecting the appropriate action for breaches of information rights

There are a number of actions the JDPA can take in the event of a breach, ranging from warnings and reprimands up to administrative fines and referrals of criminal offences to HM Attorney General. It is vital that the JOIC adopts a tailored approach when determining the most appropriate action to take in the event of a breach of information rights. This approach will take consideration of the following:

- The nature and severity of the breach or potential breach;
- The nature of the personal data affected and the level of privacy intrusion;
- The number of individuals affected, the extent of any exposure, financial, physical or psychological harm, and the degree of intrusion into their privacy;
- The vulnerability of the individual(s) affected;
- Whether the breach represents new or repeated issues, or concerns that the security measures adopted are insufficient to protect personal data;
- The gravity and duration of the breach or potential breach;
- Whether the issue raises concerns which may be systemic across a group of controllers or a business sector;
- The cost of measures to mitigate any risk, issue or harm;
- The public interest in regulatory action being taken;
- Whether another regulator, law enforcement body or competent authority is already taking action in respect of the same matter;
- Whether there are (or appears to be) any relevant aggravating or mitigating factors, including but not limited to the following:

Aggravating Factors:

» The conduct of the individual or business suggests an intentional, wilful or negligent approach to compliance;
» Ignorance of advice or warnings from the JOIC, and/or any DPO;
» The individual's or business' prior regulatory history;
» Deficiencies in the state and nature of any protective or preventative measures and technology adopted, including data protection by design/default;
» The manner in which the breach became known to the JOIC and any failure or delay by the organisation to engage with the JOIC;
» Any financial benefit gained, or costs avoided by the breach, whether directly or indirectly.

Mitigating Factors:

- Any action taken by the individual or organisation to mitigate or minimise any damage suffered by affected individuals;
- Whether the relevant individual or organisation has followed an approved or statutory code of conduct;
- Evidence that the state and nature of any protective or preventative measures and technology adopted, including data protection by design/default are at a high level;
- Early engagement by the individual or organisation with the JOIC regarding the breach.

Each case will be considered on its own merits within the context of a breach (or risk of a breach) of the DPJL or DPAJL. However, as a general principle, the more serious cases that

demonstrate a high impact, or wilful, neglectful or repeated behaviours, or a deliberate action to avoid statutory obligations can expect a more forceful regulatory response.

Conversely, those who self-report, engage and work with the JOIC to resolve issues can expect such factors to be taken into account when deciding what level of action is appropriate.

Breaches involving invasive technologies, or resulting in a high level of intrusion into the privacy of individuals can also expect a strong regulatory response, particularly where these have occurred without a full Data Protection Impact Assessment having been conducted, or where the risks have not been adequately mitigated.

When the JOIC will issue Information Notices

An information notice is a formal request for a controller, processor or individual to provide the JOIC with information, within 28 days, to assist with their investigations. In some circumstances it may be a criminal offence to provide a response which is false in any material respect.

The JOIC may serve an information notice at their discretion in any investigation/inquiry. This may include occasions where an informal request for information has not be fulfilled. Regard will be given to what action is appropriate and proportionate, and criteria including:

- the risk of harm to individuals or the potential or actual level of intrusion into their privacy by the data processing activities under investigation;
- the utility of requiring a formal response within the 28-day period;
- the utility of testing responses, by the fact that it is an offence to deliberately or recklessly make a false statement in a material respect in response; and
- he public interest in the response.

Consideration will be given to:

- the scope of the notice, that is the scope of questions or requests in an information notice;
- the length of time of the investigation. For example, it may be appropriate and proportionate to issue an information notice during a long running investigation where the questions are limited, and the response may bring the investigation closer to completion; and
- the comparative effectiveness of other investigatory powers of the JOIC.

The JOIC can consider a shorter response period in urgent cases, but generally no shorter than 7 days. In these circumstances, the JOIC will also consider:

- the extent to which urgent investigation may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy. For example, requesting an early report on a serious data security breach in order for the JOIC to advise the controller on, and validate appropriate notification to data subjects and appropriate mitigation of the breach;
- the extent to which urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing.

If a recipient of an Information Notice does not fully respond within the time period specified, the Information Commissioner will decide whether to apply for a court order requiring a response. Exceptionally the Commissioner may decide not to make such application, having regard to criteria including:

- the reasons for non-compliance with the Information Notice;
- any commitments given by the recipient to responding to the Information Notice;
- whether the information has been or is likely to be obtained from another source;
- the comparative effectiveness of other investigatory and enforcement powers of the JOIC. For example, the JOIC may decide it has sufficient evidence to move to an enforcement action in any event; and
- the public interest.

When the JOIC will exercise its powers of entry and search

The DPAJL enables the JOIC to exercise a general power of entry and search of premises where there are reasonable grounds for believing that a contravention of the DPJL or DPAJL was or is being committed on those premises.

The JOIC may choose to exercise this power of entry in circumstances where (having regard to the appropriateness of such action and the requirements of the DPAJL):

- Personal data is being processed in contravention of the DPJL and has caused, is causing, or could cause damage or distress to individuals; or
- Communications with, or information received about the controller or processor suggests that personal data is being processed in contravention of the DPJL and has caused, is causing, or could cause damage or distress to individuals; or
- The controller or processor has failed to comply with an information notice within the required timeframe.

When determining the risks of non-compliance, the JOIC will consider one or more of the factors for regulatory action. They will also consider other relevant information, such as reports by whistle-blowers, and any data protection impact assessments that may have been carried out.

Assessment of documents

Whether as part of an investigation, inquiry or other regulatory action taken, the JOIC may require access to certain documentation and information which define and explain how a controller or processor has complied with the obligations set out under the DPJL or DPAJL. This will include the governance controls in place to measure compliance. These documents may include (but are not limited to):

- Strategies
- Policies
- Procedures
- Guidance (internal and external)
- Codes of Practice
- Training logs and materials
- Protocols and frameworks
- Memoranda of understanding
- Contracts
- Privacy statements and policies
- Data protection impact assessments
- Job descriptions
- Business continuity and disaster recovery plans
- Retention schedules
- Data security policies and procedures
- Any other material relevant to the investigation

The JOIC may also need access to specified personal data or classes of personal data, and to see evidence that it is being handled in compliance with the policies and procedures which ensure compliance with the legislation. The level of access will be limited to the extent necessary to assess compliance.

This may also include access to information which:

- is subject to legal professional privilege (see below);
- has a high level of commercial sensitivity;
- is exempt information as defined by Article 27 FOIJL (information supplied by, or relating to bodies dealing with security matters); or
- is exempt from the DPJL, by virtue of a national security exemption.

The JOIC recognise that there might also be legitimate concerns about other information which relates to issues of national security, international relations or sensitive activities. In these cases, it will generally be possible to audit data protection compliance without access to such information. Where it is necessary and appropriate, the JOIC will ensure that properly vetted members of staff inspect such information.

Individuals can contact the JOIC to request that, if an assessment notice requires access to such information, this access be limited to the minimum required to adequately assess their compliance with the legislation. They may also request other access conditions. Such requests must be made within 28 days of the notice, unless the assessment is to be conducted on shorter notice, in which case, as soon as reasonably possible.

The JOIC may need to view health and social care records. If so, they will respect the confidentiality of this data, and will limit access to the minimum required to adequately assess compliance. The content will not be taken off-site, neither will it be copied or transcribed into working notes or included in any reporting of the assessment save to the extent that such is necessary to record the JOIC's investigation process and any decisions reached.

Assessments: Inspections and examinations

As part of an investigation, inquiry or other regulatory action taken, the JOIC may undertake inspections and examinations. These are key review elements of an assessment and help the JOIC to identify objective evidence of compliance, and how policies and procedures have been implemented.

These reviews of personal data, and associated logs and audit trails, may consider both manually and electronically stored data, including data stored centrally, locally and on mobile devices and media.

These reviews are used to evaluate how an organisation:

- obtains, stores, organises, adapts or alters information (e.g. policies and procedures) or personal data;
- ensures the confidentiality, integrity and availability of the data or service it provides;
- retrieves, consults, or uses the information or personal data;
- discloses personal data by transmitting or disseminating or otherwise making the data available; and
- weeds and destroys personal data.

The review may also cover management or control information, to monitor and record how personal data is being processed, and to measure how a controller meets their wider obligations under the legislation.

The review may evaluate physical and IT-related security measures, including how personal data is stored and disposed of. The review and evaluation process may take place on site as part of a discussion with staff to demonstrate 'practice', or independently by way of sampling by JOIC officers or auditors.

If information is held electronically the JOIC may require the controller to provide manual copies or facilitate direct access. Any direct access would be limited to the identified records, would only be done locally and would be for a limited and agreed time.

Data reviewed as part of the review and evaluation process, but not specifically identified in the assessment notice, may only be taken off the controller's site with the controller's permission.

Assessments: Interviews

As part of the JDPA's powers of investigation and inquiry, the JOIC may conduct interviews with relevant individuals which may consist of discussions with:

- staff and contractors;
- any processor's staff; and
- staff of relevant service providers as specified in the assessment notice.

JOIC officers will conduct interviews to develop further understanding of working practices and/or awareness of regulatory obligations. Departmental managers, operational staff, support staff (e.g. IT staff, security staff) as well as staff involved with information and information governance may be interviewed.

Where possible and practicable, interview schedules will be agreed with the controller or processor before the on-site audit. Individuals should be advised by the target organisation in advance of their required participation.

The interviewers will use questions to understand individual roles and processes followed or managed, specifically referring to the handling of personal data and its security. Some questions may cover training and awareness, but they will not be framed as a test, nor are they intended to catch people out.

Interviews may be conducted at an individual's desk or in a separate room dependent upon circumstances, and whether there is a need to observe the working environment or examine information and records. Interviews will normally be 'one-to-one', but sometimes it may be appropriate to include a number of staff in an interview – where, for example, there are shared responsibilities. Any auditors present will take notes during the interviews.

Given the nature of interviews it is not considered necessary for interviewees to be accompanied by third parties, but JOIC officers will not object where it is reasonably recommended.

Every effort will be made to restrict interviews to staff identified within the agreed schedule. However, when it becomes clear during an audit that access to additional staff may be necessary, this will be arranged with the consent of the controller. Similarly, the schedule will not prevent confirmatory conversations with a consenting third party taking place, for example where the third party is close to a desk-side discussion.

Interviews are to help in assessing compliance. They do not form part of, or provide information for, any individual disciplinary or criminal investigation. Should evidence of criminal activity by an individual emerge during an interview, the interview will be halted.

Individuals' names may be used in distribution lists and the acknowledgements sections of reports, but they will not be referenced in the body of any report. Job titles may be used where appropriate.

In the event of a criminal investigation, interviews will be held in line with Code C of the Police Procedures and Criminal Evidence (Codes of Practice)(Jersey) Order 2004. Privileged communications

The JOIC will not normally require access to information which is subject to legal professional privilege. Where such information is provided to the JOIC in connection with an investigation or inquiry, the confidentiality of this information will be respected.

When the JOIC will issue a Determination

A determination will be issued at the conclusion of an investigation where a controller or processor has been alleged to have contravened the DPJL or DPAJL. For example, this may include a breach of one of the data protection principles.

The purpose of the determination is to indicate whether or not there has been, or is likely to be, a contravention of the Law. The JDPA may also decide whether or not to impose a sanction under Article 25 of the DPAJL, or an administrative fine under Article 26 of the DPAJL.

In the case of a determination of a breach, the notice will set out:

- The specifics of the breach identified;
- The right of appeal. Part 3: Sanctions, fines and publication of regulatory actions

Penalties and Sanctions (as set out in Art.25 of the DPAJL)

PART 3: SANCTIONS, FINES AND PUBLICATION OF REGULATORY ACTIONS

Penalties and Sanctions (as set out in Art.25 of the DPAJL)

The JDPA's powers to issue a sanction or administrative fine against a controller or processor are detailed in full in Appendix 2, however it should be noted that the issuing of a sanction or administrative fine by the JDPA will be dependent upon a number of factors:

- the nature, gravity and duration of the failure;
- The intentional character of the failure or the extent of negligence involved;
- any action taken by the controller or processor to mitigate the damage or distress suffered by the data subjects;
- the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with Articles 8, 14, 15, 21 and 22 of the DPJL;
- any relevant previous failures by the controller or processor;
- the degree of co-operation with the JOIC, in order to remedy the failure and mitigate the possible adverse risks of the failure;
- the categories of personal data affected by the failure;
- the manner in which the infringement became known to the JOIC, including whether, and if so to what extent, the controller or processor notified the JOIC of the failure;
- the extent to which the controller or processor has complied with previous notices, determinations, recommendations or orders;
- adherence to any applicable approved codes of conduct or certification mechanisms;
- any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);
- whether the penalty would be effective, proportionate and dissuasive.

Before issuing a breach determination, order, or an administrative fine, the controller or processor will be notified of the intention of the JDPA to take the relevant action (the Notice of Intent). The Notice of Intent will set out the circumstances of the breach, the findings of the investigation, in the case of an order what is proposed, and in the case of an administrative fine, the proposed level of the fine and/or any rationale behind the decision to fine including its level. In the case of a breach determination or order, the grounds for and the

terms of the breach determination or order. The Notice of Intent will also detail any further requirements of the controller or processor in terms of achieving compliance with the DPJL or DPAJL. The controller or processor will have 28 days from the date of receipt of the Notice of Intent to make any written representations and JDPA will take those representations into account before finalising its decision.

Determining the amount of the administrative fine

The JDPA has the power to issue an administrative fine up to a maximum of £10million for certain breaches, however the DPAJL also states that an administrative fine must not exceed £300,000 or 10% of the organisation's global annual turnover or total gross income in the preceding financial year, whichever is the higher.

The approach to determining the amount of a fine will be on the basis of the following mechanism:

Step 1	An 'initial element' removing any financial gain arising from the breach.
Step 2	Adding an element to censure the breach based on its scale and severity, taking into account the considerations identified in Article 26(2) of the DPAJL.
Step 3	Adding in an element to reflect any aggravating factors.
Step 4	Adding an amount to act as a deterrent to others.
Step 5	Reducing the amount (save for the initial element) to reflect any mitigating factors, including the ability of the controller or processor to pay (financial hardship).
Step 6	Checking that, in all the circumstances of the case, the amount of the fine meets the requirement to be effective, proportionate and dissuasive, as set out in Art.26(3) of the DPAJL.

In general terms, the amount of the fine will be higher in circumstances where:

- vulnerable individuals or critical national infrastructure are affected;
- there has been deliberate action for financial or personal gain;
- advice, guidance, recommendations or warnings by JOIC officers and/or the organisation's DPO have been ignored or not acted upon;
- there has been a high degree of intrusion into the privacy of a data subject;
- there has been a failure to cooperate with a JOIC investigation, reprimand, determination or order; and
- there is a pattern of poor regulatory history by the controller or processor.

Late registration and payments

All controllers and processors subject to the DPJL must register with the JDPA and pay the associated fee by the last day of February each year. It is an offence for a controller or processor to fail to register with the JDPA as required. Such offences are liable to a fine.

During the first full year of the new registration process, any overdue payments will be discussed first with the controller or processor. Should the controller or processor fail to pay the charge due, any outstanding monies will be recovered as a civil debt, and if necessary through the Jersey Petty Debts Court or Royal Court, as appropriate.

Publication, openness and transparency of the JOIC

The JOIC will, as a matter of course, publish details about the volumes and types of cases it deals with. This may include details about cases which result in sanctions being levied upon controllers and processors, including administrative fines, determinations and decision notices.

In certain cases where the breach is of sufficient gravity and it in the public interest, the JDPA may determine that it is necessary to issue a public statement. The main objectives of issuing a public statement are to educate organisations and the general public, to act as a deterrent to other organisations, and to raise general levels of compliance with the DPJL and DPAJL.

If the JDPA also determines that the breach was of sufficient gravity to warrant the issuing of a fine, the controller will usually be advised, in advance of publication, of the content of that public notice.

International Cooperation

The JOIC is able to work alongside other Data Protection Authorities (DPAs) across the globe, which is essential given the extent of international data flows and the extra-territorial nature of the DPJL. These cooperation powers are set out in Articles 15 and 16 of the DPAJL. In cases involving cross-border information flows, we will liaise with other concerned DPAs to identify the most appropriate regulatory response, as well as to share information and intelligence, assist investigations, provide mutual aid and secure appropriate regulatory outcomes.

The JDPA is already a member of the following international bodies:

- The British Islands and Irish Data Protection Authorities (BIIDPA) network;
- The Global Privacy Assembly (GPA);
- The Common Thread Network (CTN);
- The Global Privacy Enforcement Network (GPEN);
- The International Conference of Information Commissioners (ICIC);
- The Conference of the Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP);

Collaborative Action

The DPJL and DPAJL legislate for certain criminal offences, for example, failing to register with the JDPA and unlawfully obtaining personal data without the consent of the relevant controller. Whilst the JOIC has the ability to investigate criminal offences, a prosecution case against an alleged offender can only be brought by HM Attorney General.

In practice, any criminal offences suspected under the DPJL or DPAJL would be referred to the States of Jersey Police for investigation, with technical assistance provided by officers of the JOIC. Similarly, the States of Jersey Police may request assistance from JOIC officers in the event they undertake an investigation of a criminal nature relevant to data protection.

In terms of regulatory activity, the JOIC may work alongside other local regulators and law enforcement bodies where data protection-related matters are identified, and where joint regulatory or investigative work is required. These may include:

- The Jersey Financial Services Commission;
- The Jersey Competition Regulatory Authority;
- The Channel Islands Financial Ombudsman;
- The Government of Jersey Customs and Immigration Service;
- The Courts.

Next steps

The JOIC's Business Plan supports this Regulatory Action and Enforcement Policy and supports the strategic plan of the JDPA. It is the intention of the JDPA to keep this policy under review and update it where necessary to reflect any changes in the legislation.

Should you have any questions over how the JDPA will mobilise their enforcement capabilities, please contact the JOIC office on 01534 716530.

APPENDIX 1

Statutory duty to investigate complaints

(Article 20 and 21 of the Data Protection Authority (Jersey) Law 2018)

The JOIC have a statutory duty to investigate complaints (Article 20 DPAJL):

(1) 20 Investigation of complaints (1) Upon receiving a complaint, the Authority must –

(a) promptly give the complainant a written acknowledgment of the receipt of the complaint; and (b) as soon as practicable and in any event within 8 weeks of receiving the complaint, determine in accordance with paragraph (2) whether or not to investigate it.

(2) The Authority must investigate the complaint unless –

(a) the complaint is clearly unfounded;

(b) the complaint is frivolous, vexatious, unnecessarily repetitive or otherwise excessive; or

(c) the Authority determines that it is inappropriate to investigate the complaint, having regard to any other action taken by the Authority under –

(i) Article 14 or 15, or

(ii) any Regulations made under Article 16.

(3) Where a complaint is investigated, the Authority must give the complainant and the controller or processor concerned –

(a) as soon as practicable, and in any event within 8 weeks of receiving the complaint, written notice that the complaint is being investigated; and

(b) at least once within 12 weeks of the notice under sub-paragraph

(a), written notice of the progress and, if possible, the outcome of the investigation.

(4) However, where the Authority considers that giving the notice within the time specified by paragraph (3) is likely seriously to prejudice the investigation, the Authority may delay giving the notice, in which case it must give the notice (including an update as to the progress of and, where applicable the outcome of the investigation) as soon as it is possible to do so without seriously prejudicing the investigation.

(5) If the Authority determines not to investigate a complaint, the Authority must give the complainant written notice of its determination and the reasons for it within 8 weeks of receiving the complaint.

(6) A notice under paragraph (4) must include information as to the complainant's right to bring proceedings under Article 31.

Similarly, the JOIC has a duty in Law to conduct an inquiry in relation to whether a controller or processor has contravened the provisions of the Data Protection (Jersey) Law 2018 (Article 21 DPAJL):

21 Inquiries

(1) The Authority may conduct an inquiry on its own initiative into the application of the Data Protection Law, including into whether –

(a) a controller or processor has contravened the Data Protection Law; or

(b) any intended processing in the context of a controller or processor, or any intended act or omission of a controller or processor, is likely to contravene that Law.

(2) An inquiry may be conducted –

(a) on the basis of information or a request received from any person or any other basis;

(b) together with, or in addition to and separately from, an investigation under Article 20.

(3) Where the Authority decides to conduct an inquiry into any matter of a kind specified in paragraph (1) (a) or (b), the Authority must give the controller or processor concerned – (a) as soon as practicable, and in any event within 8 weeks of commencing the inquiry, written notice of the nature of the inquiry; and (b) at least once within 12 weeks of the notice under sub-paragraph (a), written notice of the progress and, if possible, the outcome of the inquiry.

(4) However, where the Authority considers that giving the notice within the time specified by paragraph (3) is likely seriously to prejudice the inquiry, the Authority may delay giving the notice, in which case it must give the notice (including an update as to the progress of and, where applicable the outcome of the inquiry) as soon as it is possible to do so without seriously prejudicing the inquiry.

(5) Nothing in this Article limits – (a) an individual's right to make a complaint under Article 19, or (b) the duties of the Authority under Article 20.

APPENDIX 2

Information Notices and audits

Para 1, Schedule 1 of the Data Protection Authority (Jersey) Law 2018) and Para 7, Schedule 1 of the Data Protection Authority (Jersey) Law 2018)

1 Power to issue information notice

(1) The Authority may require any controller or processor to give the Authority any information that the Authority considers necessary for a purpose specified in sub-paragraph

(2) by issuing the controller or processor ("the recipient") a notice (an "information notice"). (2) The purposes referred to in subparagraph (1) are –

(a) to determine whether or not to investigate a complaint;

(b) to determine whether or not to conduct an inquiry;

(c) for the purpose of an investigation or inquiry;

(d) to make a determination or an order, or take any other action, under any provision of Part 4; or

(e) to determine whether or not to exercise any other power conferred on the Authority by this Law.

(3) An information notice must include –

(a) a statement of the purpose in sub-paragraph (2) for which the notice is issued;

(b) a description of the information required by the Authority;

(c) a statement of the Authority's reasons for requiring that information; and

(d) a statement of the form and manner in which, and the period within which ("compliance period"), the recipient must give the information to the Authority.

(4) A compliance period must not be shorter than 28 days beginning on the date on which the notice was issued.

(5) Despite sub-paragraph (4), the Authority may specify a compliance period shorter than 28 days but not shorter than 7 days beginning on the date on which the notice was issued, but in this case the Authority must include in the information notice a statement of its reasons for specifying that shorter period.

(6) A recipient of an information notice must comply with the notice.

(7) A recipient is not required by virtue of this paragraph to furnish the Authority with any information in respect of –

(a) any communication between a professional legal adviser and a client in connection with the giving of legal advice to the client with respect to the latter's obligations, liabilities or rights under this Law or the Data Protection Law; or

(b) any communication between a professional legal adviser and a client, or between such an adviser or client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Law or the Data Protection Law and for the purposes of such proceedings.

(8) In sub-paragraph (7), references to a client of a professional legal adviser include references to any person representing such a client.

(9) A recipient is not required by virtue of this paragraph to furnish the Authority with any information if to do so would, by revealing evidence of the commission of any offence other than an offence under this Law, expose the recipient to proceedings for that offence.

(10) The Authority may cancel an information notice by written notice served on the person on whom the information notice was served.

7 Power to conduct or require data protection audits

(1) The Authority may –

(a) conduct a data protection audit of any part of the operations of the controller or processor; or

(b) require the controller or processor to appoint a person approved by the Authority to –

» (i) conduct a data protection audit of any part of the operations of the controller or processor, and

» (ii) report the findings of the audit to the Authority.

(2) The Authority must specify the terms of reference of any audit carried out under sub-paragraph (1).

(3) The controller or processor concerned must pay for an audit required under sub-paragraph (1)(b).

APPENDIX 3

Statutory provisions relating to sanctions and administrative fines

(Articles 25, 26 and 27 of the Data Protection Authority (Jersey) Law 2018)

Article 25 of the DPAJL sets out the sanctions available to the JDPA in the event of a breach having been identified:

25 Sanctions following breach determination

(1) If the Authority makes a breach determination against a controller or processor, the Authority may by written notice to the controller or processor ("the recipient") take all or any of the following sanctions against the recipient – (a) issue a reprimand to the recipient; (b) issue a warning to the recipient that the intended processing or other act or omission is likely to contravene the Data Protection Law; (c) make an order under paragraph (3).

(2) Paragraph (1) does not limit the Authority's power to impose an administrative fine under Article 26 in the case of a contravention of the Data Protection Law.

(3) The Authority may order the recipient to do all or any of the following –

(a) bring specified processing operations into compliance with the Data Protection Law, or take any other specified action required to comply with that Law, in a manner and within a period specified in the order;

(b) notify a data subject of any personal data breach;

(c) comply with a request made by the data subject to exercise a data subject right;

(d) rectify or erase personal data in accordance with Article 31 or 32 of the Data Protection Law;

(e) restrict or limit the recipient's processing operations, which may include – (i) temporarily restricting processing operations in accordance with Article 33 of the Data Protection Law, (ii) ceasing all processing operations for a specified period or until a specified action is taken, or (iii) suspending any transfers of personal data to a recipient in any other jurisdiction; and

(f) notify persons to whom the personal data has been disclosed of the rectification, erasure or temporary restriction on processing, in accordance with Articles 31 to 33 of the Data Protection Law.

(4) Nothing in paragraph (3)(d), (e) or (f) limits paragraph (3)(c).

(5) An order under subsection (3) may, in relation to each requirement in the order, specify –

(a) the time at which, or by which, the requirement must be complied with; and

(b) the period during which the requirement must be complied with (including the occurrence of any action or event upon which compliance with the requirement may cease).

(6) The Authority may revoke or amend an order under paragraph (3) by giving written notice to the person concerned.

(7) A recipient in respect of whom an order is made under paragraph (3) must comply with the order within any time specified for its compliance. (8) A person who contravenes paragraph (7) is guilty of an offence.

Articles 26 and 27 of the DPAJL sets out the provisions available to the JDPA in relation to administrative fines:

26 Administrative fines

(1) Subject to Article 27 the Authority may order a controller or processor to pay to the Authority an administrative fine for any of the following –

(a) 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 Data Protection Law is a person duly authorized to give consent to that processing in accordance with that provision;
(b) breach of any duty or obligation imposed by Article 7 of, and any provision of Parts 3, 4 or 5 of, the Data Protection Law;
(c) processing personal data in breach of any other provision of Part 2 or 6 of the Data Protection Law; or
(d) transfer of personal data to a person in a third country or international organization in contravention of Article 66 or 67 of the Data Protection Law.

(2) In determining whether or not to order a fine and, if ordered, the amount of the fine, the Authority must have regard to –
(a) the nature, gravity and duration of the contravention of the Data Protection Law, taking into account the nature, scope and purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
(b) whether the contravention was intentional or negligent;
(c) any action taken by the person concerned to mitigate the loss, damage or distress suffered by data subjects;
(d) the degree of responsibility of the person concerned taking into account technical and organizational measures implemented by the person concerned for the purposes of any provision of the Data Protection Law;
(e) any relevant previous contraventions by the person concerned;
(f) the degree of cooperation with the Authority, in order to remedy the breaches and mitigate the possible adverse effects of the contravention;
(g) the categories of personal data affected by the contravention;
(h) the manner in which the contravention became known to the Authority, in particular whether, and if so to what extent, the person concerned notified the contravention to the Authority;
(i) where an order under Article 25(3) has previously been made in respect of the person concerned with regard to the same subject-matter, compliance with any measures required to be taken by the order;(j) compliance or non-compliance with code or evidence of certification in respect of the processing concerned; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the contravention.

(3) In ordering any fine, the Authority must take into account the need for fines to –
(a) be effective;
(b) be proportionate; and
(c) have a deterrent effect.

(4) An order imposing a fine –
(a) must specify the date by which the fine must be paid; and
(b) may provide for the fine to be paid by instalments of any number and amounts and at any times specified in the order.

(5) The Authority may, of its own motion or on the application of the person concerned, vary –
(a) the amount of a fine; or
(b) the number, amounts and times of the instalments by which the fine is to be paid.

(6) The Authority may publish the name of the person concerned and the amount of the fine in any manner it considers appropriate.

(7) The Authority may recover a fine as a debt owed and due to the Authority by the person concerned.

(8) A fine imposed on an unincorporated body by an order of the Authority must be paid from the funds of the body.

(9) Nothing in this Article authorizes the Authority to order a public authority other than one falling only within paragraph (k) of the definition of "public authority" in Article 1(1) of the Data Protection Law to pay a fine.

(10) Any fine paid to or recovered by the Authority forms part of the annual income of the States.

(11) In this Article – "fine" means an administrative fine ordered under paragraph (1); "person concerned" means the controller or processor against whom an administrative fine is ordered.

27 Limits on administrative fines

(1) Subject to paragraphs (2) and (3) an administrative fine ordered against a person –
(a) for any matter specified in Article 26(1)(a) and (b), must not exceed £5,000,000;
(b) for any matter specified in Article 26(1)(c) or (d), must not exceed £10,000,000.

(2) 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.

(3) 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.

(4) Where a person contravenes several provisions of the Data Protection Law in relation to the same processing operations, or associated or otherwise linked processing operations, the aggregate of the administrative fines issued against the controller or processor in respect of those processing operations must not exceed the limit specified under paragraph (1)(a) or, if applicable to any such contravention, paragraph (1)(b).

(5) The Minister may, by Order, amend any monetary amount set out in this Article and Regulations may amend Article 26 and other provision of this Article.

MORE INFORMATION

Jersey Office of the Information Commissioner
2nd Floor
5 Castle Street
St Helier
Jersey JE2 3BT

Telephone number: +44 (0) 1534 716530
Email: enquiries@jerseyoic.org