JOB DESCRIPTION

JOB TITLE:	Caseworker – Entry Level
AREA:	Compliance and Enforcement
REPORTS TO:	Compliance and Enforcement Manager
BAND:	4

JOB PURPOSE:

To work as part of the Casework Team responsible for investigating reports of potential data breaches across a range of data controllers and processors on the Island to determine the appropriate way forward. Applying persuasive compliance wherever possible by engaging with a range of stakeholders to build relationships and offer advice, education and awareness on Data Protection laws, whilst supporting them to make changes to align with evolving regulations. Where an offence is committed, work closely with members of the Casework Team and follow the Casework process, to ensure a consistent approach to enforcement.

ACCOUNTABILITIES AND RESPONSIBILITIES

Responsible for a range of routine casework procedures and practices. Providing basic advice and resolving common problems. Works within organisational policies and guidelines, and is expected to refer to more senior caseworkers for advice when necessary to deliver in the following technical areas:

COMPLIANCE & ENFORCEMENT

- Provide guidance and advice for general data protection enquiries.
- Respond to routine complaints and enquiries across a range of data controllers and processors.
- Deal with regulatory breaches, including but not limited to; self-reported data breaches, registration breaches and security breaches. Where possible, through means of persuasive compliance, working with stakeholders to take remedial action.
- Support the organisation's audit programme to ensure good practice and compliance with the relevant laws.
- Proactively identify cases where a data protection audit may be required, supporting on-site compliance visits to data controllers and data processors, assessing policies and procedures for legal compliance.
- Support audits within the JOIC's audit programme, where appropriate, ensuring good practice and compliance with the relevant laws.

- Where necessary, assisting with detailed investigations / inquiries into potential offences committed under the laws.

- Obtain the best possible evidence of offences committed under the Law, assist in preparing report summaries and case files. Assist with preparing information and enforcement notices, as appropriate.

- Support with the review of appeals under the Freedom of Information Law.

- Ensure current knowledge of data protection and freedom of information issues, such as changes to the law, emerging technologies and current affairs. Assist with reviewing data protection impact assessments on new programmes, laws and information technologies.

- Maintain accurate casework records, ensuring full compliance with casework policies and procedures.

- Assist in gathering measurable data where possible, to provide evidence of team and organisational performance.

- Assist with enquiries and the administration of registrations.

- Support the organisation's business planning process and contribute or lead on deliverables as appropriate.

QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

- Intermediate knowledge, equating to a Higher National Certificate, Technician, or other diploma or equivalent with experience in research and analysis and demonstrable accuracy and attention to detail.

- The ability to acquire a good working knowledge of a range of aspects of the Data Protection (Jersey) Law, Data Protection Authority (Jersey) Law and the Freedom of Information (Jersey) Law and other related legislation.

- The capability and willingness to undertake the 'Practitioners Certificate in Data Protection' qualification, or equivalent and apply this knowledge on the job.

- Excellent interpersonal skills with the ability to build relationships and effectively communicate through written, face to face or virtual interactions.

- Computer literate with willingness to learn about emerging technologies and associated impact on data protection (e.g. cyber-crime, blockchain).

DESIRABLE

- Previous experience of working in a regulatory environment carrying out compliance and enforcement activities. A proactive and professional approach to work, where others typically guide the day-to-day tasks.

- Experience of auditing as part of an internal or external audit team.

- Knowledge of emerging technologies and associated impact on data protection (e.g. cyber-crime, blockchain).

- The ability to present to groups, to educate and raise awareness of data protection.