information commissioner

Barrantagh Fysseree

Regulatory Policy

Contents

Introduction

In an era of ubiquitous computing and global communications it has have become increasingly important to uphold and protect the information rights of individuals. The Isle of Man Information Commissioner's Office has been established as the independent supervisory authority with regulatory powers to do so in the Isle of Man.

In our experience, the majority of Controllers and Processors in the Island do seek to respect the information rights of individuals and comply with their obligations when processing personal data. This also means that when compliance issues arise most are resolved without the need for formal enforcement action.

However, when enforcement action is necessary, the Information Commissioner ('Commissioner') has been provided with significant powers which range from giving a warning or reprimand for minor contraventions to banning processing and imposing a penalty of up to £1 million for the most serious contraventions.

The purpose of this policy is to explain the Commissioner's approach to regulatory action.

This policy explains how fair, proportionate and timely action will be taken with a view to ensuring that individuals' information rights are upheld and personal data is processed in accordance with law and is properly protected.

This Policy will be reviewed and evaluated and updated to reflect any amendments to legislation and evolving best practice.

Isle of Man Data Protection Legislation

The Isle of Man's *'data protection legislation'* consists of:-

- Data Protection Act 2018 ('DPA2018')
- Data Protection (Application of the GDPR) Order 2018 ('*Applied GDPR*')
- Data Protection (Application of the LED) Order 2018 *('Applied LED'*)
- GDPR and LED Implementing Regulations 2018 ('*Implementing Regulations'*)

Certain enforcement powers in the Implementing Regulations also apply to:-

- The Unsolicited Communications Regulations 2005 *('UCR'*)

The Commissioner also has responsibility for:-

- Freedom of Information Act 2015 (*FOIA*);

and

- Code of Practice on Access to Government Information 1995 ('*Code of Practice'*)

This policy applies to regulatory action taken under data protection legislation or the UCR.

Statutory provisions requiring guidance

The following Implementing Regulations contain provisions where the Commissioner must, or may, issue guidance: -

Regulation 92: Guidance about privileged communications

Regulation 95: Guidance about fees

Regulation 115: Fixed penalties for non-compliance with charges regulations

Regulation 118: Guidance about corrective action

Regulation 145: Guidance about codes of practice

This policy, with the exceptions noted below, provides guidance on how:-

- powers to give information notices, assessment notices, enforcement notices, and penalty notices will be exercised (*Reg 118*);
- other enforcement functions will be exercised *(Reg 145);* and
- privileged communications obtained or accessed when carrying out statutory functions will be used or disclosed. *(Reg 92)*

Note:

1. *Guidance about fees (regulation 95) requires the written concurrence of the Treasury and will be published separately when appropriate.*

2. *Regulations requiring a controller or processor to pay charges to the Commissioner have not been made by Council of Ministers under regulation 96. Consequently, there is no guidance for the Commissioner to produce and publish under Regulation 115.*

International co-operation and action

The Commissioner will also take action in line with international co-operation obligations under both the GDPR and Council of Europe Convention 108.

In cases involving cross-jurisdictional data flows, the Commissioner will liaise with other relevant supervisory authorities to identify and agree the most appropriate regulatory response, including identifying any lead authority or other concerned supervisory authorities.

The Commissioner will share information with other supervisory authorities to assist investigations, provide mutual aid and secure appropriate regulatory outcomes.

The Commissioner is the designated competent authority for Council of Europe Convention 108 and a member of :

- British Islands and Irish Data Protection Authorities network (UK, Ireland, Bermuda, Cyprus, Gibraltar, Guernsey, Jersey, Malta and Isle of Man)
- Common Thread Network *(Commonwealth countries*) www.commonthreadnetwork.org
- Global Privacy Enforcement Network www.privacyenforcement.net
- Global Privacy Assembly www.globalprivacyassembly.org
- International Conference of Information Commissioners *(FOI)* https://www.informationcommissioners.org/

Policy Objectives

The objectives of the Commissioner are to:-

1. Encourage compliance through the promotion of good practice and provision of advice and guidance.

2. Respond promptly and effectively to personal data breaches and contraventions of data protection legislation, with particular attention to those that:-
    a. involve sensitive information,
    b. adversely affect large groups of individuals, or
    c. impact vulnerable individuals.

3. Be effective, proportionate and dissuasive in the application of sanctions, reserving the most significant sanctions:-
    a. for persons who repeatedly or wilfully fail to comply with the data protection legislation, or
    b. where regulatory action serves as an important deterrent.

Approach to Regulatory Action

Advice and Guidance

The Commissioner will continue to encourage compliance and promote good practice.

The Commissioner provides compliance advice and guidance to controllers and processors as well as advice and guidance to individuals about their rights and how to exercise them.

The Commissioner's website www.inforights.im provides the primary source of advice and guidance as any other advice or guidance, for example provided by phone or at a meeting or seminar, could be misunderstood or misinterpreted.

The Commissioner does not give legal advice.

Determining the appropriate regulatory action

Each matter will be considered and reviewed on its merits. Appropriate regulatory action will be determined in light of the information available to the Commissioner at any given time and within the context of any contravention or risk of contravention.

In general, contraventions with more serious, high-impact, intentional, wilful, neglectful or repeated factors can expect stronger regulatory action.

Contraventions involving new or invasive technology, or a high degree of intrusion into the privacy of individuals, without undergoing a proper Data Protection Impact Assessment or taking subsequent appropriate action to mitigate high risk, or, where required, failing to consult with the Commissioner, can also expect stronger regulatory action.

When deciding whether, and how, to respond to an issue, the following may be considered:-

- the nature and seriousness of the contravention or breach;
- the categories of personal data affected, with particular regard to any special category personal data or criminal conviction data that may be involved;
- the risk posed to any individual and the degree of any intrusion into an individual's privacy;
- the gravity and duration of the contravention or breach;
- the number of individuals affected;
- whether the issue raises new or repeated issues, or concerns that security measures are not protecting the personal data;
- the measures required to mitigate any risk to individuals;
- the public interest in regulatory action being taken (for example, as an effective deterrent against similar contraventions).

Aggravating or mitigating factors, which may also be considered, include for example:

Aggravating Factors

- whether the attitude and conduct of the individual or organisation suggests an intentional, wilful or negligent approach to compliance or unlawful business or operating model;
- whether advice, warnings, or guidance from the Commissioner, or, where relevant the Data Protection Officer, has not been followed;
- any adverse regulatory history;
- the vulnerability, if any, of the individuals affected;
- the nature of any preventative measures and technology available, including data protection by default and design;
- the manner in which the Commissioner became aware of the issue and any failure, or delay, to inform the Commissioner; and
- any financial benefits gained or financial losses avoided by the relevant individual or organisation, directly or indirectly.

Mitigating factors

- early notification by the relevant individual, or organisation, of the issue;
- unilateral action taken to mitigate or minimise any damage;
- steps taken to prevent a reoccurrence;
- full and proper co-operation with the Commissioner;
- whether an approved or statutory code of conduct has been followed; and
- the prior use of available preventative measures and technology.

Enforcement Powers

In summary, the Commissioners' enforcement powers include:-

- an information notice which requires information to be provided to the Commissioner within a specified time;
- an assessment notice which requires a controller or processor to provide access to premises, equipment, information etc. within a specified time;
- the power or entry and inspection, if necessary, under a warrant;
- giving a warning where non-compliance is likely;
- giving a reprimand for infringements;
- giving enforcement notices that require specific action to be taken to rectify non-compliance or prevent potential breaches;
- requiring urgent compliance with an information, assessment, or enforcement notice;
- giving a penalty notice up to £1,000,000;
- applying to court for an order requiring compliance with an information notice, assessment notice, an enforcement notice or a penalty notice;
- prosecuting criminal offences.

Information Notices

An Information Notice is a formal notification requiring the provision of information to the Commissioner, within a specified time frame, to assist with any investigation. An Information Notice may, depending on the circumstances, be given to any person. Further detail, including statutory provisions, is provided in the Information Notices guidance note.

In deciding to give an Information Notice, regard as to whether that action is appropriate and proportionate may include consideration of:

- the risk of harm to individuals, or the level of intrusion into their privacy that may be posed by the events or data processing under investigation;
- the value to the investigation of the information sought;
- the burden upon the recipient; and
- the necessity of requiring a response within a defined time period.

When deciding the period for compliance with an Information Notice, in particular whether or not to issue an 'urgent' Information Notice, regard as to what action is appropriate and proportionate may also include consideration of:

- the extent to which urgent investigation may prevent or limit the risk of harm to individuals or intrusion into their privacy. For example requesting an early report on a personal data breach in order to advise the controller whether to notify data subjects and other appropriate mitigation of the breach.
- whether an urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing;
- the additional burden upon the recipient of having to comply with a notice urgently;
- the impact on the rights of the recipient, i.e. can the Commissioner justify the need to obtain information under an urgent Information Notice prior to an appeal being heard by the Tribunal.

Information sought

The information that can be sought by an Information Notice is not limited to personal data and may include access to information in policies and procedures, records of processing activities and the governance controls in place. Although not exhaustive this could include access to information contained in:

- Strategies
- Policies
- Procedures
- Staff Guidance
- Codes of practice
- Training material

- Protocols
- Frameworks
- Memoranda of understanding
- Contracts
- Privacy statements
- Privacy impact assessments
- Control data, and
- Job descriptions

Access may be required to information which:

- is special category personal data;
- is subject to legal professional privilege (see below);
- has a high level of commercial sensitivity; or
- is subject to a national security certificate,

but will only be sought when it is necessary for the investigation and only to the extent necessary to assess compliance, for example to ascertain if an exemption from the right of access can be applied.

The confidentiality of this data will be respected and will not be included in any report.

Privileged communications

In general, the Commissioner will not require information subject to legal professional privilege to be provided. However, occasions arise where access to information which is subject to a claim of legal professional privilege is required in order to establish, for example, whether that personal data is exempt from the right of access to personal data.

The Commissioner may not require the provision of privileged legal advice or litigation advice where communications between a professional legal adviser and the adviser's client are in connection with the client's obligations, rights or liabilities under the data protection legislation, or proceedings, including contemplated proceedings, under the data protection legislation.

Non-compliance with an Information Notice

If a recipient of an Information Notice does not comply with the Information Notice then the Commissioner can certify the failure to the High Court who can deal with matter as a contempt of Court.

Before doing so, the Commissioner may consider:

- any reasons for non-compliance with the Information Notice;
- any commitments given by the recipient to fully respond to the Information Notice;

- whether the information can be obtained from another source;
- whether using other enforcement powers, for example, whether sufficient information has been obtained to give an Enforcement Notice; and
- the public interest.

The Commissioner will also consider whether or not to issue a Penalty Notice.

Assessment Notices

An Assessment Notice is a formal request given to a controller or processor requiring access to premises, equipment, staff, documentation and information in order to assess compliance with the data protection legislation. Further detail, including statutory provisions, is provided in the Assessment Notices guidance note.

In deciding whether to give an Assessment Notice the following may be considered:-

- any indication or information that personal data are not being processed in compliance with the data protection legislation, for example, result of a data protection impact assessment, personal data breach reports, reports from whistle blowers, etc.
- any failure to respond to an Information Notice;
- to verify compliance with an Enforcement Notice;
- the likelihood of damage or distress to individuals;
- the value to the investigation of the information sought; and
- the burden upon the recipient.

When deciding the period for compliance and in particular whether or not to issue an urgent Assessment Notice, the Commissioner may consider:-

- the extent to which an urgent investigation may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy;
- the extent to which an urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing;
- the scope of the assessment;
- any additional burden in having to comply with a notice urgently;
- the impact on the rights of the recipient of urgent access without the opportunity for an appeal to be heard by the Tribunal.

Inspection and examinations

Inspections and examinations help identify evidence of compliance, and how policies and procedures have been implemented in practice. A review of the processing of personal data, and associated logs and audit trails assist the understanding of how the controller or processor:-

- obtains, stores, organises, adapts or alters information 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.

A review may include access to management/control information to monitor and record how personal data is being processed, and to measure how a controller or processor meets their wider obligations under the legislation.

A review may also evaluate physical and technical security measures, including how personal data is stored and disposed of.

Interviews

Interviews may occur during an Assessment and consist of discussions with:

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

Such interviews assist with the assessment of compliance, the understanding of working practices and the extent of awareness with regulatory obligations.

Where possible, identification of the relevant level and grade of staff to be interviewed will be agreed and arranged with the controller or processor prior to commencement of an Assessment. Prior agreement and arrangement will permit the controller or processor to advise each individual of their participation and ensure they are available for interview at the relevant time. If it becomes necessary to interview further staff then this will be arranged with the controller or processor.

Interviews will normally be 'one-to-one', but sometimes it may be appropriate to include a number of staff in an interview, for example, where there are shared responsibilities. If desired, interviewees may be accompanied by a third party.

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. Arranged interviews do not preclude confirmatory conversations with other persons during an Assessment, for example, a conversation with a member of staff during an observed processing activity may occur.

Questions asked during an interview are intended to help understand the processes and procedures being followed and the individual's role in those processes. Where questions are asked about an individual's training and awareness they will not be framed as a test.

Interviews 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.

Notes will be taken during interviews.

Non-compliance with an Assessment Notice

If a recipient does not comply with an Assessment Notice then the Commissioner may apply for a court order.

The Commissioner, having taken into account:-

- any reasons given by the recipient for non-compliance;
- any commitments given to respond to the Assessment Notice;
- whether the information has been or is likely to be obtained from another source

may decide not to make an application.

The Commissioner will also consider whether or not to issue a penalty notice.

Enforcement Notices

Enforcement Notices may be given where a type of failure described in regulation 106 has occurred, for example, a controller has infringed one of the data protection principles, or failed to comply with data subject rights. Further detail, including statutory provisions, is provided in the Enforcement Notices guidance note.

The purpose of an Enforcement Notice is to require action to be taken to bring about compliance with the data protection legislation and/or remedy a breach.

Enforcement Notices will usually be appropriate where specific correcting action or preventative action is required. Although this is not an exhaustive list, an Enforcement Notice may be given when:-

- there has been a failure to meet information rights obligations or timescales for them (e.g. failure to comply with subject access requests);
- where there is an ongoing data security issue;
- there is a need to communicate a data security breach to those who have been affected by it; or
- there is a need for correcting action by a certification body or monitoring body to ensure that they meet their obligations.

The notice will set out:

- who is required to take the action and why;
- the specifics of the action to be taken;
- how to report that the action has been taken;
- the timescales that apply for that action; and,
- any appeal / challenge process that applies.

When deciding whether to issue an Enforcement Notice, factors such as those set out above, and any mitigating or aggravating factors, will be considered.

In general, the timescales set out in an Enforcement Notice will reflect whether timely action can prevent further contraventions, the severity and scale of any contravention, or the time required to implement any correcting measures or technology.

Consideration will be given as to whether urgent action is appropriate and proportionate having regard to criteria including:

- the extent to which such urgent action may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy. For example requiring a controller to take action to protect personal data from a security breach;
- the scope of the Enforcement Notice; and

- the additional burden or impact upon the recipient in having to comply with an urgent Enforcement Notice within the period specified.

Non-compliance with an Enforcement Notice

Failure to comply with an Enforcement Notice will result in the Commissioner applying for a court order.

The Commissioner will also consider whether or not to issue a penalty notice.

Penalty Notices

A Penalty Notice is intended to act as an effective and dissuasive deterrent and ensure compliance with the legislation and information rights obligations. Penalties must, therefore, provide an appropriate sanction. Further detail, including statutory provisions, is provided in the Penalty Notices guidance note.

In deciding whether to give a penalty notice **and** the amount of the penalty, the following factors may be considered:

- the nature, gravity and duration of the contravention;
- 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;
- any previous failure by the controller or processor;
- the degree of co-operation with the Commissioner, 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 Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;
- the extent to which the controller or processor has complied with any previous notices;
- adherence to 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.

Each case will be assessed objectively on its own merits but, in general, Penalty Notices will be reserved for serious cases including, for example, wilful, deliberate or negligent acts, or repeated infringements of information rights obligations, causing harm or damage to individuals.

Notice of Intent

Prior to giving a Penalty Notice, the Commissioner will advise the controller or processer of the intention to do so by issuing a notice of intent (NOI). The NOI will set out the circumstances of any infringement, investigation findings, the proposed penalty and a rationale for the penalty.

At least 21 calendar days will be given for representations to be made about the imposition and level of the proposed penalty.

Exceptionally, at the Commissioner's discretion, representations may be permitted to be made

orally. If an organisation or individual thinks that the circumstances warrant oral representations, this should be explained in their written representations. Before agreeing to do so, the Commissioner will need to be satisfied that oral representations will add to the regulatory process.

Amount of penalty

The maximum penalty is £1,000,000.

In general, the amount of a penalty will be higher where:

- vulnerable individuals or critical national infrastructure are affected;
- there has been deliberate action for financial or personal gain;
- advice, guidance, recommendations or warnings 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;
- there has been a failure to comply with a notice;
- there is a history of non-compliance.

The amount of a penalty will be determined by applying:-

1. an 'initial element' that removes any financial gain from the infringement;
2. an element to censure the contravention based on scale and severity;
3. a further element to reflect any aggravating factors;
4. if necessary, a further amount to provide a deterrent effect;
5. a reduction to reflect any mitigating factors, and any ability to pay.