Douglas Borough Council responses to
Consultation questionnaire on Draft Data Protection (GDPR) Bill

Child consent age

The Council of Ministers has considered views on the designated age of a child in the context of Article 8 of the GDPR (Regulation 11).

The Council of Ministers has taken the view that the age, below which consent must be sought for the provision of information society services, is 13 years. This is in line with the approach being taken by the UK and is the lowest age permitted by the GDPR (the standard being 16 years).

Question 1. Do you agree with this decision?

Response: Yes – the age should be in line with the UK approach of 13 years

Certification

Article 42 of the GDPR (Regulation 17) encourages the establishment and use of data protection certification mechanisms to show that the processing operations of controllers and processors comply with the GDPR.

The Isle of Man Regulations make provision for the Information Commissioner or a *national accreditation body* to accredit a person as a certification provider. The term 'national accreditation body' is not yet defined. It could refer to a body in the UK, a body in the Isle of Man or both.

Question 2. Should the Isle of Man recognise national accreditation bodies?

Response: Yes – open to non-Island bodies so that larger companies with fixed processes, complying with standards in one jurisdiction, need not undergo separate accreditation in the Island.

Transfer Principles

Under Article 44 of the GDPR (Regulation 74), transfers of personal data to a third country or international organisation, including those not subject to an adequacy decision, are subject to conditions set out in Articles 45 and 46 of the GDPR.

These provisions have been adapted to an Isle of Man context, giving the Information Commissioner powers to give approval to transfers where an adequacy decision is not in place.

Question 3. Do you agree with the proposed adaptations?

Response: Yes, because they give greater flexibility in international transactions and the Information Commissioner can ensure that even if no adequacy decision is in place, there is still sufficient protection of data.

Binding Corporate Rules

Binding corporate rules are internal rules adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection.

Under Article 47 of the GDPR (Regulation 75), the Information Commissioner shall approve binding corporate rules, subject to a series of conditions as laid out in that Article. The GDPR sets out a consistency mechanism under Article 63 of the GDPR. The Council of Ministers has taken a pragmatic view in respect of the consistency mechanism and has removed the requirement for that mechanism to be used.

Question 4. Do you support this approach to binding corporate rules?

Response: Yes – the Council supports this approach

Expanded Information Commissioner Powers

The Information Commissioner will have an expanded range of powers and sanctions and an updated role. These include:

a. Consideration and endorsement of appropriate guidance and codes of practice and the power for the Commissioner to issue guidance or codes of practice (Regulations 89-94).

b. The application in full of the powers in Article 58 of the GDPR (Regulations Part 7), together with Schedules 4 (powers of entry and seizure) and 5 (penalties) including the ability to request information from data controllers, enter premises and a series of investigative and corrective powers. The Information Commissioner is also given a set of advisory and authorisation functions. Such functions are subject to appropriate safeguards within the proposed legislation, including effective judicial remedy and due process.

c. At present, the Information Commissioner is designated as the Supervisory Authority for the purposes of the GDPR and the LED (Regulations 83 and 84). The Council of Minsters has agreed that in future, the Office of the Information Commissioner should become a Statutory Board under the Statutory Boards Act 1987.

d. The process of notification to the Information Commissioner of the processing of personal data by a controller or processor is retained. The Information Commissioner will retain a register of data controllers and processors. It is intended this will be expanded to include the name of the designated Data Protection Officer for an organisation.

e. The Information Commissioner will continue to charge a fee for notification under the new legislation. The fees payable will be prescribed by fees regulations. One proposal for the way that fees are charged is to introduce a tiered fee scale so that smaller businesses pay less than larger businesses or those which process a large amount of personal data.

Question 5. Do you agree that the powers afforded to the Information Commissioner are proportionate?

Response: Yes

Question 6. Do you agree that the Information Commissioner's Office should ultimately become a Statutory Board?

Response: Yes; the unit may need further resourcing to undertake the additional responsibility and it should operate as an arm of Government.

Question 7. Do you agree with the retention of the notification process for the Information Commissioner?

Response: Not in its current form whereby notification does not include any demonstration of how data is being protected. All data processors should be required to demonstrate what data they are processing, and how it is protected, when they submit their notification. However there could be exemption for very small organisations, particularly charities, in order not to overburden them.

Question 8. Do you agree with the retention of the fee process for notification?

Response: Yes; fees should be charged in order to finance, at least in part, the expanded role of the Information Commissioner's Office.

Question 9. Do you support a tiered fee structure based on the size of an organisation and the amount of records processed?

Response: A tiered structure is desirable in order not to penalise smaller businesses; if feasible it should be based on the number of records processed instead of size of business.

Question 10. Do you have any additional comments about the role of the Information Commissioner?

Recommended response: The role of the Information Commissioner is increasing significantly under the Bill and the Council's concern would be that the Office is correctly resourced to manage with the increasing responsibilities, especially in the early months of the new legislation where the Commission is more likely to be busy with additional requests from data subjects and companies. The example of additional responsibility in Article 36 in relation to Data Protection Impact statements, although there is an 8 week response period this is likely to hold up many organisations and cause frustration that may lead to organisations not engaging.

Administrative fines

In Article 83 of the GDPR the limits of administrative fines are set at *up to* 10,000,000 EUR or 2% of annual turnover for undertakings as lower level fines for certain infringements and *up to* 20,000,000 EUR or 4% of annual turnover for undertakings as upper level fines for certain infringements. The proposed legislation (Regulation 119 and Schedule 5) contains a maximum discretionary penalty of up to £1million.

Question 11. Is the maximum level of penalty (administrative fine), proposed at £1,000,000 an effective, proportionate and dissuasive remedy for the Isle of Man?

Response: Yes – effective and proportionate.

Criminal offences

Criminal offences are included in the draft Regulations on the same basis as the Data Protection Act 2002, providing for a fine of up to £10,000 on summary conviction and an unlimited fine on information in the High Court (Regulation 145).

Question 12. Do you agree with the decision to retain the sanctions for criminal offences from the Data Protection Act?

Response: Yes – retain the sanctions

Question 13. Are there any transitional provisions the Isle of Man Government should consider to help make sure organisations are ready for compliance with the new legislative provisions in GDPR? (For example a defined grace period)

What transitional provisions should the Isle of Man Government consider?

Response: Following the introduction of the legislation it would seem harsh to fine a company early in its operation on the basis of (a) the complexity and understanding of the legislation and (b) the resource required and length of time needed to comply with the new regime. In the Council's experience to date there has been little clarity on many issues and the reality is that many of these more difficult questions will only be answered once the legislation is in operation.

It is also felt that the Information commissioner has a significantly increased role and the reality of being able to manage the influx and increase in workload will be difficult. Many of the Articles now refer to increased guidance from the Information Commissioner, specifically in relation to personal impact statements (Article 36). It would be beneficial to provide a risk based rollout where areas of the Act are prioritised, e.g. the reporting of a breach within 72 hours should be a requirement on Day 1. The requirement for international agreements such as Binding Corporate Contracts also needs to be in place from Day 1 so that the Island can continue doing business with the EU. The legislation cannot be partly implemented but what must be in place and enforced on Day 1, and what elements can be activated later in a planned rollout, needs to be clarified.

More guidance and advice is needed from the Information Commissioner: currently requests are met with advice to seek advice from a legal adviser. However law firms do not have practical experience and that situation will be exacerbated when the new Regulations are applied.

Exemptions including public interest exemptions

Article 23 of the GDPR enables the Island to introduce derogations to the GDPR in certain situations. We can introduce exemptions from the GDPR's transparency obligations and individual rights, **but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure** in a democratic society to safeguard:

- national security
- defence
- public security
- the prevention, investigation, detection or prosecution of criminal offences
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security

- the protection of judicial independence and proceedings
- breaches of ethics in regulated professions
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention
- the protection of the individual, or the rights and freedoms of others
- the enforcement of civil law matters

The legislation also gives powers in respect of exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

- freedom of expression and freedom of information
- public access to official documents
- national identification numbers
- processing of employee data
- processing for archiving purposes and for scientific or historical research and statistical purposes
- secrecy obligations
- churches and religious associations

An initial list of proposed exemptions is included in the draft Regulations.

Question 14. Are these exemptions sufficient?

Response: Yes.

Final thoughts

Question 15. Do you wish to add any further comments on the proposed legislation and regulations?

Response: Only that **t**he Council is concerned about the provision for Government and its officers to be protected from sanction in Regulation 153. Every individual must be dealt with according to the law and there is no reason to exclude anyone simply because they are part of, or employed by, Government. No.