EU General Data Protection Regulation (GDPR)

Consultation paper – summary of responses and analysis 2018

The consultation ran from 23 January to 5 March 2018 inviting views on the proposed Orders and Regulations, addressed in particular to private, public and third sector organisations which process, or are likely to process personal data.

The Cabinet Office received 57 responses to the consultation.32 organisations and 25 individuals responded.

- 18 gave permission to publish their response in full
- 26 gave permission to publish anonymously
- 13 did not give consent to publish on the consultation hub.

Clear themes emerging from the consultation responses include:

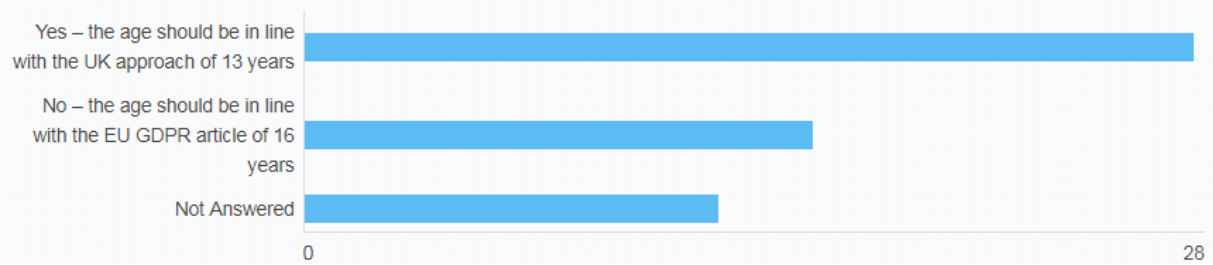
- Openness and transparency
- Need for guidance and good practice information
- Concerns around divergence from UK position
- Ensuring that sanctions / fines etc. are enforceable

There were also specific comments aimed at clarifying specific wording and definitions in articles and regulations.

Thank you to everyone who took the time to submit their views and responses to this consultation.

1. Child consent age - Article 8 of the GDPR (Regulation 11).

The consultation stated that Council of Ministers supported the age below which consent must be sought for the provision of information society services of 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).



Respondents to this question were divided, with 28 agreeing with the UK approach of 13 years and 16 supporting the EU age of 16. 13 respondents did not answer the question.

Those who support the EU approach of 16 years, said they did so because of the need to protect children, and that those under 16 are not experienced or aware enough to know what they are consenting to.

- 'Until the age of 16 a parent/guardian should be giving consent. 13 is too young for many children to make an informed decision when giving consent.'
- 'I believe that parents are better placed to protect children than they are themselves. It should be a clear defence if a parent can show that they were not consulted.'
- 'I have a very real concern that we are treating our children as older than they are in some matters and sidelining parental involvement and responsibility for them.'

Those who supported the UK approach of 13 years, said that children were technologically aware earlier on, and were capable of independent decisions at this age. The Chamber of Commerce response also agreed with adopting the age of consent in line with the UK.

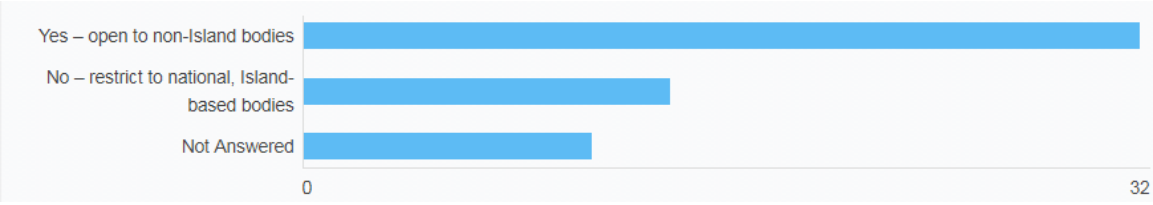
- 'A growing body of evidence from across the world is telling us that no matter where they are from, more and more children are relying on digital tools, platforms and services to learn, engage, participate, play, innovate, work or socialise - therefore, childrens' consent should be sought from the age of 13'
- 'At 13 to 16 years, a person is old enough to make decisions and actions independently of their parents'
- 'adopting an age of consent in line with the UK approach makes sense'
- 'This should also assist practically in aligning with the pre-existing approach applied by the major social media players e.g Facebook'

Those who did not select either age either told us that it did not impact on their business area, or that the Isle of Man should choose the age that is most appropriate.

- 'I have not [sic] particular thoughts on using either age. However, I would ask how this compares with other ages of majority and whether lowering the age would expose children to additional risks to their personal data arising out of inexperience or naivety?'

2. Certification - Article 42 of the GDPR (Regulation 17)

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.



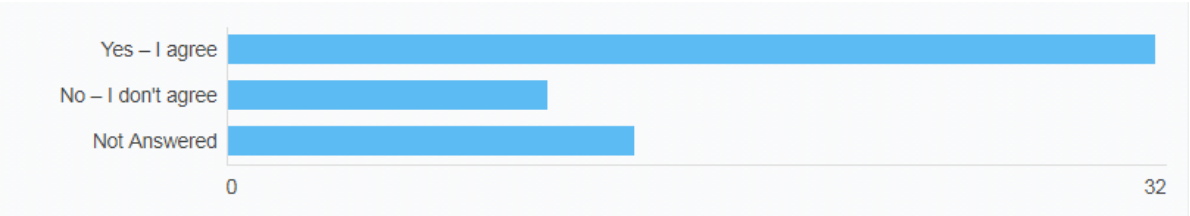
32 respondents thought that the Isle of Man should recognise national accreditation bodies (non-Island bodies). 14 wanted to see this restricted to national, Island-based bodies, and 11 did not answer this question.

Those who thought national accreditation bodies should be recognised said:

- 'The alternative seems costly and time-consuming, for little obvious benefit to the Isle of Man'.
- 'The UK have more organisations training in this space that will need (under the UK Bill) to be approved by the Secretary of State'
- '[should be..] 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.'
- 'suggest that this is restricted to IOM plus UK providers.'
- 'By recognising bodies in both the Isle of Man and the UK…there is greater scope for consistency of quality to the testing and accreditation of certification providers; however, keeping the accreditation bodies within the Isle of Man has the potential to create new income streams for appropriately qualified local organisations.'
- ' the Isle of Man should recognise national accreditation bodies outside the Isle of Man, where those standards are considered acceptable, because it is not practical to restrict recognition to Island-based bodies.'

3. Transfer Principles - Articles 45 and 46 of the GDPR

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 45 and 46. 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.



32 agree with the proposed adaptations and 11 disagree. 14 did not provide a yes/ no answer to this question.

Reasons given for agreeing include:

- 'In extreme circumstances, e.g. the prevention of terrorist activities, it may be necessary to exchange information quickly and in good faith.'
- 'Would approval be required on each individual occasion of the transfer of personal data or would one approval be sufficient for further transfers? What are the timescales for approval?'
- '…it should speed up the timeframe for approval if we can submit them directly to our own regulator (who we have a relationship with and are likely to understand our business)'

- 'International nature of business on the Island needs to be able to transfer outside of adequate jurisdictions, assistance from the ICO with this is beneficial.'
- 'The adaptations appear to offer the protection that is needed to ensure that personal data is being adequately protected and only shared when right and proper'.
- 'where an adequacy decision is not in place, giving the Information Commissioner powers to give approval to transfers of personal data to a third country or international organisation appears a pragmatic solution'.

Those who disagreed said:

- 'Too much power for the Information Commissioner'
- 'Security of personal data should remain within the country
- 'Reference to transfers and adequacy under Applied GDPR should be limited to EU citizen data and take their cue from their adequacy decisions. All other data transfers should not reference the EU but be subject to recommendation of adequacy by the ICO that should be added to a specific Non-EU adequacy list appended to this legislation. This ensures independence in non-EU matters'.
- 'We need to ensure that we are able to rely on EU Adequacy decisions to avoid the disruption of current and future data flows to/from the Isle of Man'.

Following the publication of the draft Order to implement GDPR, it was noted that the entirety of Article 45 had been deleted, when in fact Article 45(1) should remain in line with the adaptations proposed in the text of the consultation. As such, Article 45(1) will be reinstated in the draft Order.

4. Binding Corporate Rules - Article 47 of the GDPR (Regulation 75)

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. 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 removed the requirement for the consistency mechanism to be used.

37 support this approach **to binding corporate rules**, saying:

- 'Since BCRs facilitate the transfer of data within groups of companies, this point will never apply to an entity solely based in the Isle of Man. Whatever mechanism we adopt needs to be in line with the EU to enable BCRs to be adopted as quickly and efficiently as possible by groups of companies that include Isle of Man entities. It is not clear at present how this will be achieved given that the consistency mechanism at Article 63 cannot apply to the Isle of Man, as it is not part of the EU'.
- 'We support the approach of removing the need for the consistency mechanism to be used in all cases, provided that it does not impact upon the Island's vital adequacy status. '

7 do not support this approach, with some respondents saying this requires more clarity.

- 'this is the means by which intra-company transfers happen today and there is actually the perverse requirement for ICO review because of lack of clarity as to what rules apply in what case. What should be clear is that these rules (within the context of GDPR) should not increase uncertainty and also not increase ICO workload – so clarity is required.'

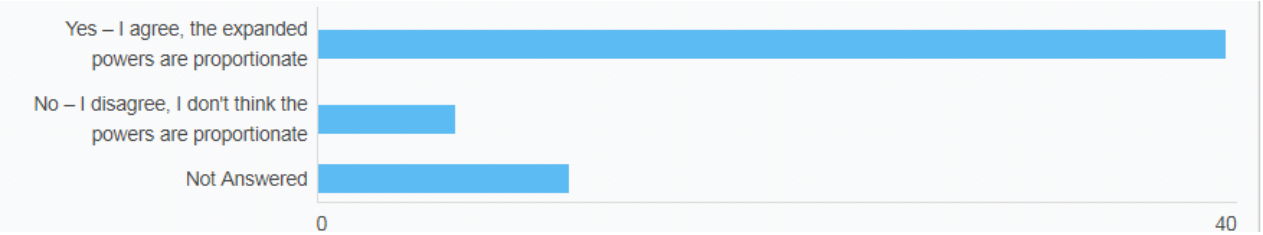
13 respondents did not provide a yes / no response.

5-10. Expanded Information Commissioner Powers

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

- Consideration and endorsement of appropriate guidance and codes of practice and the power for the Commissioner to issue guidance or codes of practice
- 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.
- Advisory and authorisation functions subject to appropriate safeguards within the proposed legislation, including effective judicial remedy and due process.

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

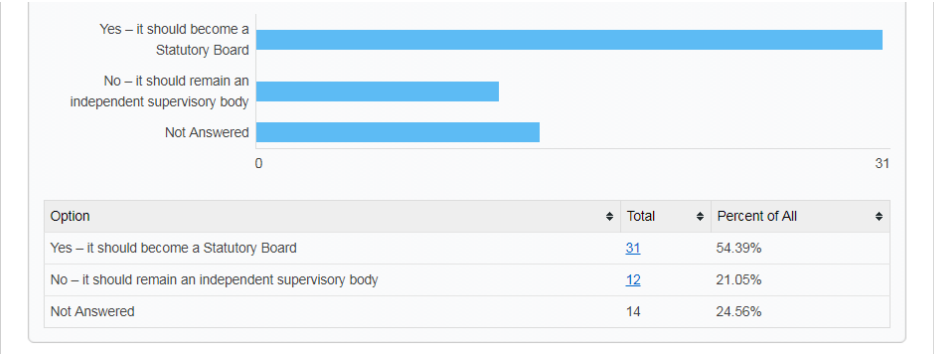


40 respondents agreed. 6 did not agree. 11 did not provide a 'yes / no' answer.

- 'It is reasonable and proportionate that the Information Commissioner should issue codes of practice and guidance on data protection matters'.

Question 6. Information Commissioner's Office as Statutory Board

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.



Option	Total	Percent of All
Yes – it should become a Statutory Board	31	54.39%
No – it should remain an independent supervisory body	12	21.05%
Not Answered	14	24.56%

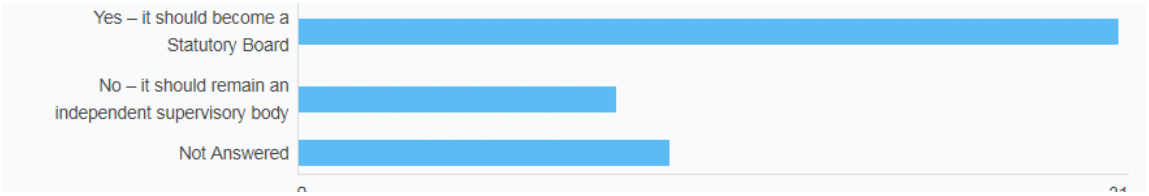
31 agreed that the Information Commissioner's Office should become a Statutory Board. 12 did not agree. 14 did not provide a yes/no answer.

- 'The Information Commissioner's Office must be beyond the influence of government, given its role to also regulate government's compliance with the applied GDPR and applied LED. We are however concerned about the lack of resource currently given to the Information Commissioner's Office.' IOM Chamber of Commerce
- 'Yes, but only if NOT chaired by a political member of the Board'

7. Notification process

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.

31 respondents agree with the retention of the notification process for the Information Commissioner. 12 did not agree. 14 did not provide a yes/no answer.



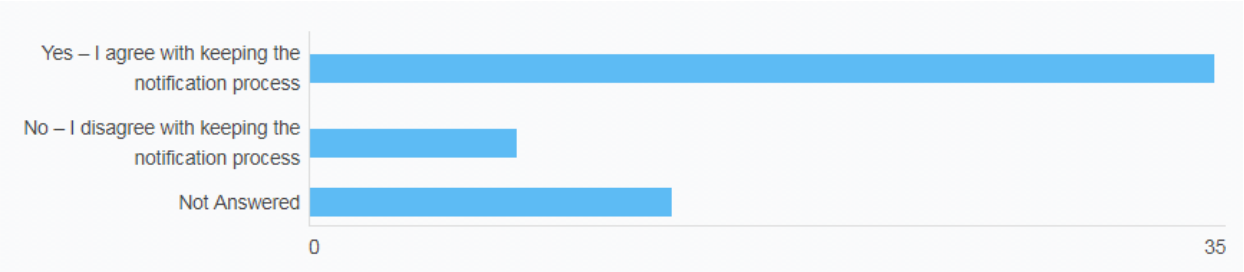
Comments included:

- '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'.
- 'it is noted that notification will require the name of the data protection officer. it is our understanding that not all data controllers or processors will be required to have a data protection officer'
- 'A notification process seems sensible, but it should not require excessive detail'.

- 'In principle yes, however further details are needed on how this would work in practice'.
- 'Retaining a notification process would seem unnecessary, and this is a confusing message for members who had been told that there is no notification requirement under the GDPR.'
- 'If the Notification were restricted to providing name and address of controller/processor together with their allocated Data Protection contact person, this response would change to "Yes, we agree"'

8. Fee process for notification

In the regulations as proposed, 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.

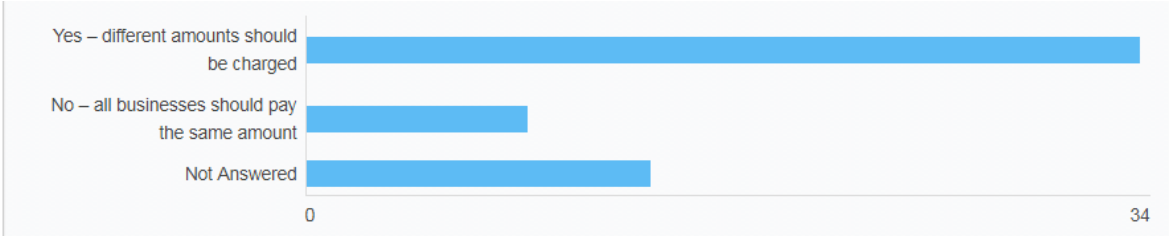


35 agreed with the retention of the fee process for notification. 8 disagreed.

Some comments suggested that without details for the fee structure some respondents said that they found it difficult to comment. Comments from later in the survey showed that some respondents felt that there were already significant expenses associated with implementing GDPR and fees were an unnecessary additional burden.

9. Tiered fee structure

The majority of respondents (34) were in favour of a tiered fee structure based on the size of an organisation and the amount of records processed. 9 thought that all businesses should pay the same amount. 14 did not provide a yes/no answer.



- 'the size of an organization does not always have a direct bearing on the volume or nature of the personal data it processes'.
- '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.'
- 'if a notification requirement is retained, members will not wish to fall foul of the legislation because of a prohibitively expensive fee, particularly given that significant expenditure will be required to meet the other requirements of the legislation.'

10. Additional comments about the role of the Information Commissioner

A number of responses highlighted the need for the role to remain independent from Government, and for there to be transparency and accountability, avoiding conflict of interest (actual and perceived).

- 'Must be adequately supervised.'
- 'The ICO should remain an independent supervisory body, as an independent surely this would be open, transparent and free from outside interference?'
- 'There needs to be independence between government and the Information Commissioner, to avoid the perception of conflict and to comply with Article 51. The is especially important as the IC's role will include supervising FoI.'
- 'we are concerned about the lack of resources given to the Information Commissioner's Office.'
- 'There must be scrutiny from outside the Island. There needs to be more than internal reviews'
- 'The powers are also unclear in some areas and should be clarified.'

Several respondents felt that the Information Commissioner must be approachable, and able to provide advice to smaller organisations who don't always feel that they can approach the ICO.

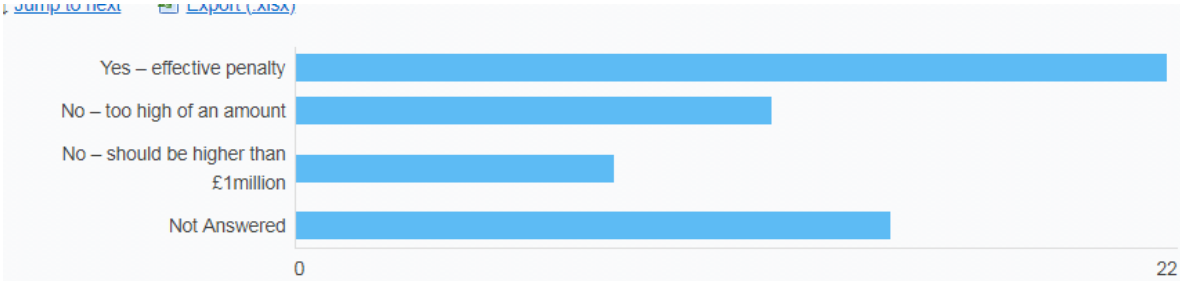
Several commenters were concerned about lack of resources for the Information Commissioners' Office particularly as proposals indicate an enhanced role for the ICO in sharing guidance and good practice. Others made comments about funding, and that it should be a self-funding role. One was concerned about checks and balances, and another about ensuring impartiality.

11. 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?



Option	Total	Percent of All
Yes – effective penalty	22	38.60%
No – too high of an amount	12	21.05%
No – should be higher than £1million	8	14.04%
Not Answered	15	26.32%

22 respondents thought this was an effective penalty. 12 thought the amount was too high. 8 thought it should be higher than £1million. 15 did not provide a specific response to this question. Comments included:

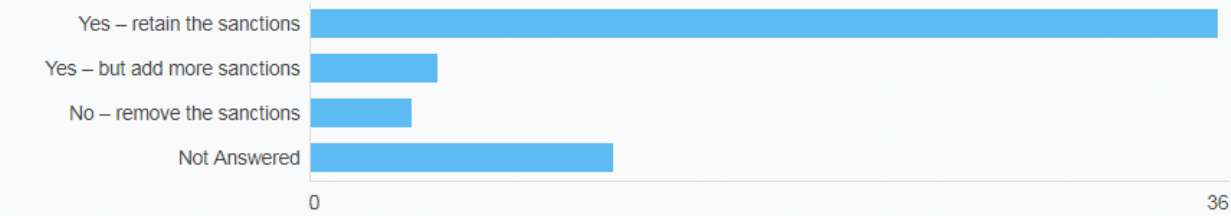
- 'A maximum penalty is just that: a maximum. There is discretion to levy a fine below this amount, and we would expect any fine to be effective, proportionate and dissuasive to the recipient of the fine and so take into account their size and revenue.'
- 'It is not clear that the maximum fine for the Isle of Man has been limited to £1 million, given the wording in Regulation 119 (1)(a). We consider that the limit of £1 million is too low, given the size and nature of some of the entities based in the Isle of Man, and that the Information Commissioner should have the ability to levy a higher fine if it is appropriate in the circumstances to do so'.
- '£1m is an effective level of penalty within the private sector. However, both Public Authorities and small local third sector organisations would be severely affected by this level of fine.'
- 'Fines and Penalties are mentioned in at least 4 different Regulations…These need to be made clearer and either combines or moved to once section. At present they appear to imply that multiple fines are possible'.
- 'the practicalities and implications of charging significant financial penalties to public bodies should be fully considered – notably the source and destination of such funds as well as the impact on taxpayers'
- 'It is not clear that the maximum fine for the Isle of Man has been limited to £1 million, given the wording in Regulation 119 (1)(a)'

Following the consultation, it will be necessary to clarify the maximum penalty with wording in Regulation 119(1)(a), which will be set out in the final draft of the Implementing Regulations.

12. 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?



Option	Total	Percent of All
Yes – retain the sanctions	36	63.16%
Yes – but add more sanctions	5	8.772%
No – remove the sanctions	4	7.018%
Not Answered	12	21.05%

36 agreed with retaining the sanctions. 5 agreed with retaining the sanctions and adding more. 4 agreed that sanctions should be removed and 12 did not provide a yes/no answer.

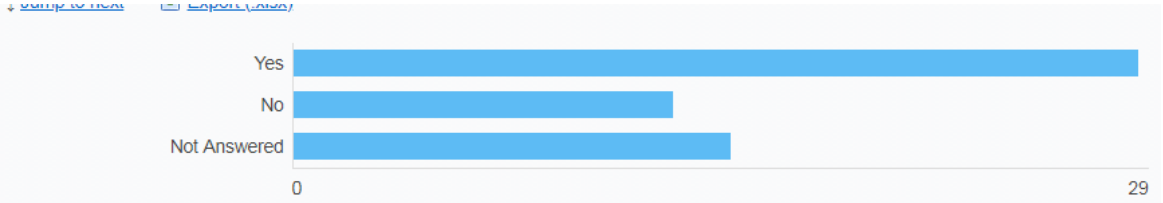
Comments include:

- 'Add further sanctions to include imprisonment for criminal offences'
- 'Criminal offences but not genuine error'
- '…these should be re-written as minimum sanctions, not maximum - human thinking will always be that the maximum will not be applied to me and to word things in this way is no real deterrent'.
- 'sanctions should act as an effective deterrent, not just a "slap on the wrist". Even low-level breaches should therefore be subject to a sanction of sufficient significance to truly deter any repeat of the behaviours leading to the breach/offence.'
- 'I think that there should be fewer sanctions. a £10,000 fine is out of the reach of most normal people. In most cases, naming and shaming ought to suffice.'

If more – then for what level of offence

No specific responses were received on this particular question.

13. 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)



Option	Total	Percent of All
Yes	29	50.88%
No	13	22.81%
Not Answered	15	26.32%

29 respondents agreed that some transitional arrangements might be needed.

Those who said yes agreed that a grace period could be helpful, of 6-12 months. Those who disagreed with this thought that 'grace periods will encourage organisations to put off compliance'.

- Legacy systems were also suggested for exemption.
- Brexit mentioned in response to this question.
- 'Any grace period could only apply to local businesses which are not caught in the extra-jurisdictional scope of the GDPR. We support a grace period for such businesses but are concerned the limited applicability of such a grace period could be misinterpreted, and entities to which the GDPR does apply delay their preparations as a result'.

What transitional provisions should the Isle of Man Government consider?

13 respondents did not think transitional arrangements were necessary or appropriate.

Those who responded 'no' said that they thought there had been enough advance warning that GDPR would be coming in, and that transitional arrangements weren't necessary. Several respondents also felt that the Isle of Man had lost its advantage by not continuing to be ahead in implementing GDPR.

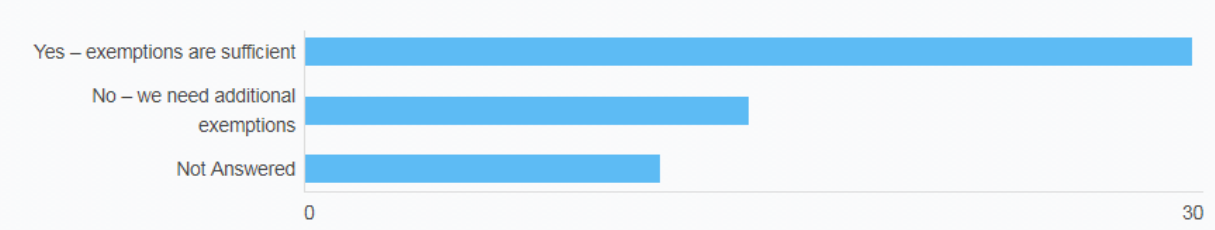
- 'warnings with a specific period to rectify'
- 'Whilst we welcome the sentiment of the 'grace period' offered in respect of consents and information to be provided to data subjects under paragraph 2 of schedule 11, there is no scope in the GDPR for transitional provisions beyond the previous two years since GDPR was enacted'
- 'a defined grace period for data controllers of 3 years to allow for sufficient time to await the potential impacts of Great Britain's exit (Brexit) from the European Union and the EU as a whole. Data Controllers will need sufficient time to digest the new legislation and see how it is applied in practice in the EU and post Brexit?'
- '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.'

14. Exemptions including public interest exemptions - Article 23 of the GDPR

This enables the Island to introduce derogations to the GDPR in certain situations. The Isle of Man 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. An initial list of proposed exemptions are included in the draft Regulations. These include processing that relates to e.g. freedom of expression and freedom of information, public access to official documents and processing of employee data.



Option	Total	Percent of All
Yes – exemptions are sufficient	30	52.63%
No – we need additional exemptions	15	26.32%
Not Answered	12	21.05%

30 respondents considered these exemptions sufficient. 15 respondents said that the exemptions were not sufficient.

Additional exemptions suggested were:

- Trust companies 'a trustee will need an express exemption from having to comply with Article 5(1)(a) in such circumstances to ensure that the trustee can legitimately avoid such a disclosure to a beneficiary who may for good reason have no knowledge of the trust - the beneficiary may for example be too young or may be a vulnerable adult and therefore it may not be appropriate for them to have knowledge of the trust' and 'We think it would be prudent to include an exemption for Trust Companies to permit access to beneficiary information'
- Life assurance
- Archiving purposes in the public interest – this should be clearly defined (response from UK Archive & Records Association)'The spirit of the GDPR is that large private sector organisations that seek to exploit personal data solely for commercial gain – for example in the social media space or data mining space - should not be allowed to 'badge' themselves as 'archives' and seek to use the 'public interest' purpose to evade their obligations under GDPR.'
- Modification orders – health, social work, education, adoption services social care. Wording to include 'social work' specifically rather than solely 'social care'.

Some respondents thought there should be fewer exemptions. Others suggested removing statutory boards from exemptions in certain areas.

- 'the law must apply equally to everyone. This means that every data controller must be subject to the same sanctions. It is, therefore, fundamentally wrong that the Departments and Statutory Boards are proposed to be exempted under the GDPR
- 'there shouldn't be as many exemptions as there are already, ie, I don't see why churches and religious organisations are exempt'

It was acknowledged following consultation that there are various exemptions included in the UK Bill, at Schedules 2 to 4, that were not included in the draft of the implementing regulations and as such it is proposed to include them, with some modifications. Those which cannot be included in the main implementing regulations due to time constraints will be dealt with as separate regulations in the next phase of regulations.

15. Further comments on the proposed legislation and regulations

A number of themes were identified in the additional comments in response to the consultation as follows:

- **Clarity and definition** - 6 comments highlighted the importance of making the explanation of GDPR requirements simpler and easier to read, and some requested clarity on definitions and/or cross referencing with GDPR and LED definitions which would make the Orders and Regulations easier to read
- **Risks to small organisations** - 3 comments highlighted the risks to smaller organisations and charities – eg the skills and capacity to implement in the required timescales without experience or knowledge/guidance required or resource implications
- **Timing** - 2 comments mentioned that they considered the Manx legislation to be rushed in comparison to other jurisdictions, and two responses were unsure why the

Implementing Regulations would be in force on 1st May 2018, a date which is earlier than the GDPR or LED requires (being 25th and 6th May 2018 respectively). Some comments mentioned that the timing of the repeal of the Data Protection Act 2002 was not clear, and asked whether this should be repealed by the primary legislation rather than in secondary Orders

- **Consultation style** - 2 comments mentioned that the consultation was not easy to respond to didn't cover all of the appropriate questions
- **Enforcement** - 3 comments queried enforceability of regulations
- **Subject access requests** – one comment made explicit provision for SARs
- **International reputation** – One comment raised a concern regarding the international reputation of the Isle of Man and in particular risks to its adequacy if the law did not implement GDPR appropriately
- **Codes of Practice and Guidance** – two comments thought that additional requirements upon the Information Commissioner to publish guidance was unnecessary, and one suggested that the Information Commissioner could continue to publish guidance where necessary, i.e. as a discretionary power to do so rather than a mandatory requirement
- **Support from Cabinet Office** – one comment made reference to the roll out of the Freedom of Information project by Cabinet Office both pre and post the implementation of the Freedom of Information Act 2015, and highlighted the value of templates and guidance documents which would be welcomed for GDPR
- **Differences in approach** – some comments highlighted concerns about divergence of approach, commenting that a difference of approach to the UK, Jersey or Guernsey, or indeed modifying the GDPR for the purposes of domestic law might risk compliance and/or adequacy
- **Membership of the EU** – In respect of the Implementing Regulations, three responses suggested confusion might be caused following the use of the 'deemed' membership of the EU and thereby treating the Isle of Man as a Member State of the EU for the purposes of the reading of the Implementing Regulations (this is a reference to how to read the Regulations, and the Isle of Man could not legislate for itself to be part of the EU).
- **Guidance and advice** – some consultation responses asked questions about how the GDPR might apply to that organisation operationally (for example in the areas of processing, retention and responding to Subject Access requests).
- **Application to the Crown** – some responses mentioned that Regulation 153 appeared to follow the UK but could not apply as drafted due to the differences in the Isle of Man Government and how it is constituted with separate legal entities. The position is intended to be the same in the new draft of the Implementing Regulations, and so this will be clarified in the final draft.

Finally, general comments highlighted some typographical errors, missing words or cross referencing. Thank you for highlighting these, giving the opportunity for the re-drafted final form legislation to be made both consistent and accurate.

Conclusion

The response to the consultation suggested broad support for the policy proposed within the specific questions set out, as follows:-

- Lowering the age of consent for a child to age 13 for the provision of information society services;
- Including both on and off Island national accreditation bodies in respect of article 43 of the GDPR;
- Retaining provisions for international transfers to an adequate country pursuant to Article 45(1) of the GDPR;
- Support for binding corporate rules, but without the need for the consistency mechanism to be used, by making it a discretionary power for the Information Commissioner to approve binding corporate rules. This is proposed as an interim step until the effects of Brexit and how these might work in practice is known. The requirement to use the consistency mechanism will be removed since the Information Commissioner could not apply this in the manner that the Articles 63-67 of the GDPR set out, as the Isle of Man is a third country;
- Support for expanded and enhanced powers of the Information Commissioner, including administrative fines and penalties, becoming an independent statutory board, and payment of a tiered fee for notification;
- Penalties for administrative fine at a maximum of £1,000,000 as an effective, proportionate and dissuasive penalty;
- Retaining sanctions for criminal offences on a similar basis as those set out in the Data Protection Act 2002, whilst acknowledging the spirit and intention of the GDPR in its fundamental aim to ensure compliance, rather than enforcement. This has led to some slight differences in the enforcement provisions, but provision of the powers to the Information Commissioner to effectively monitor and enforce compliance where necessary;
- Provision of transition periods akin to those set out in the Data Protection Act 2002, and in particular providing a transition period for the new notification period of 12 months;
- Agreement with exemptions provided subject to clarification in respect of health, education and social work, and addition of further exemptions for archiving purposes in the public interest, for trusts and for the land registry. Additional exemptions will also be included to ensure there is no conflict between anti-money laundering and countering the financing of terrorism requirements for screening and the GDPR.

Further general comments were provided requesting support and advice, clarity on certain provisions or definitions, highlighting risks particularly to smaller organisations, and concerns about the timing of the legislation and the impending deadline, together with the risk to the Isle of Man's adequacy decision. The Cabinet Office acknowledges these concerns and is working together with the Information Commissioner to provide training and awareness sessions for as many representative groups and associations as possible.

The consultation showed that there remains some uncertainty as to the legal mechanism and the rationale behind the approach, which the Cabinet Office will continue to address via its website and media releases, in collaboration with the Information Commissioner's Office, to ensure that the Isle of Man is ready for the significant culture and regulatory change the GDPR and the LED will require.

Next steps

Stage 1 – Enacting new primary legislation – the Data Protection Act 2018

The Bill has now completed its passage through the House of Keys and the Legislative Council with no amendments. The second and third reading of the Bill together with the clauses stage in Legislative Council was passed on 27th March 2018, and as such the necessary steps are being taken to obtain Royal Assent to the Bill.

Details of the passage of the Bill through the Houses can be found here: http://www.tynwald.org.im/business/bills/Pages/default.aspx and the Official Reports of the Proceedings (Hansard)

Stage 2 – Implementing Orders and Regulations

If the Bill receives Royal Assent, the secondary legislation will then be laid before Tynwald, which will in the first instance include:

- The Orders which import the GDPR and the LED with local modifications so that they read as domestic law; and
- Implementing Regulations, which will preserve the elements of the existing Data Protection Act 2002 and implement the critical elements of the GDPR and LED into domestic law in order that those provisions remain essentially equivalent, to avoid any risk to the Island's adequacy status.

Stage 3 – Regulations

Following the Stage 2 implementation of GDPR and LED as domestic law, together with the regulatory regime behind the critical elements, the consultation response has shown a clear requirement for further regulations which will deal with the detail on:-

- Additional subject access and fair processing modifications and exemptions (in a way which is similar to the existing Orders made under the Data Protection Act 2002;
- Notification regulations and fee structure;
- Any other transitional or additional provisions required.

Stage 4 – Guidance, Codes and Accreditation

The GDPR and the LED separately set out areas where jurisdictions may provide for policies, guidance, codes of practice, certification and accreditation. Not all such matters need to be covered in legislative provisions, and can be dealt with administratively. Following the publication of the Implementing Regulations, together with any additional Stage 3

regulations set out above, work will be underway, to produce any codes, guidance or practice which the GDPR or LED set out.

The Future of Data Protection Legislation

The legislative programme includes the drafting of a new Data Protection Bill in the 2019/2020 schedule which will permit the Island to make this short term responsive and flexible legislative arrangement into primary legislation once we have had a full opportunity to review the impact of the withdrawal of the UK from the EU (Brexit), and the impact of GDPR and the LED both on the Island and in other jurisdictions.

We asked, you said, we did

We Asked

The Cabinet Office asked for feedback on proposed changes to the Isle of Man's new data protection framework between 23rd January and 5th March 2018. The proposed enabling Data Protection Bill, with secondary legislation comprising draft Orders implementing the GDPR and the LED, and implementing regulations were published with the consultation, along with a number of questions on various areas of fundamental policy.

You Said

The consultation attracted over 50 responses in total, from a number of categories of respondent, including businesses, industry associations, local authorities and individuals, in addition to Government Departments and other associations. The majority of responses supported the specific questions set out, and set out further comments on diverse areas from drafting and typographical issues, areas requiring clarification or further regulation, or specific issues such as modifications and exemptions.

We Did

The Cabinet Office has considered all of the comments and suggestions received. A paper providing full details of the consultation feedback, and the Cabinet Office's responses has been published on the Isle of Man Government's Consultation Hub. The enabling Bill completed its passage through the House of Keys and Legislative Council, and as a direct result of the consultation, parts of the draft GDPR and LED Orders, together with significant parts of the Implementing Regulations have been amended.

The revised Orders and Implementing Regulations as amended are due to be laid before Tynwald at its May sitting. There will be further development of additional secondary legislation and such guidance, codes or otherwise as required to ensure proper implementation of the GDPR and the LED.

Responses received from organisations

Alliance of Isle of Man Compliance Professionals (AICP)

Appleby

Castletown Medical Centre

Cayman National

Central Registry

Crowe Morgan Management Limited – highlighting Jersey regulations on subject access exemptions

Department for Environment Fisheries and Agriculture (DEFA)

Department of Health and Social Care - Children and Families

Department of Infrastructure

Douglas Borough Council

DQ Advocates Limited

Equiom Group

HSBC PLC Isle of Man branch

Financial Intelligence Unit (FIU)

IOM Association of Corporate Service Providers

Isle of Man Chamber of Commerce

Isle of Man Constabulary

Manx ICT Association (MICTA)

Manx Utilities Authority

Michael Parish Church

Old Mutual International

Price Waterhouse Coopers LLC

Santander International

STEP Isle of Man

SMP Partners Limited

Zedra Trust Company (Isle of Man) Limited