Q&A session – GDPR Conference 24th January 2018

QUESTIONS	RESPONSES AND FURTHER READING
Enforcement and sanctions - What happens if Treasury breach? - What benefit can there be in fining a public authority when funds are staying in government, but the department will lose some of its operational ability with that money? - So if DHSC get fined £1m, it goes back to treasury? - Will public sector be fined at the same level as the private sector? - Where will the fines from the IOM ICO go? - Which SAs will be responsible for fining multinationals, particularly if we are able to interpret our	• Fines under the GDPR are set out in Article 83 which provide that infringements of the provisions shall be subject to administrative fines up to the levels set out in that Article (10m/20m EURO, or 2/4% of annual turnover). • Administrative fines will be administered by the ICO, and ultimately all penalties paid in fines will be receipted by the Treasury • As such, the consultation seeks views on what sanctions could be imposed upon public sector (to avoid a circular payment from one Government Department to another) • It is proposed that all infringements in the public or private sector should have sanctions with some parity – taking into account legislative mechanism, and much like other areas of legislation which creates offences and liability at both personal and corporate level, it is expected that a range of sanctions be implemented • The Isle of Man needs to ensure that its range of sanctions are effective, proportionate and dissuasive as required by the GDPR • Personal liability for individual officers would remain for example where an officer was reckless or intentionally misused information. • The Isle of Man ICO cannot be a lead supervisory authority since the Isle of Man is not a member state in its own right. • The designation of the lead supervisory authority and to which jurisdiction a particular organisation might be subject to will depend upon circumstances of the case, including the main establishment of the controller/processor, and where the central organisation is based, and where processing occurs and decisions as to that processing are made. • In the hypothetical example of a German Supervisory Authority, whilst there would be an element of co-operation between the Isle of Man ICO and the German Supervisory Authority, it is anticipated that the German Supervisory Authority would take the lead supervisory authority role. • Other supervisory authorities could issue fines under their own legislative regimes accordingly.

own tiers of fines? - Manx Controller selling to Germany breaches EU & IOM GDPR - will the IOM ICO be able to take the lead supervisory role or will EU & IOM supervisor investigate/fine? - Can other supervisory bodies impose penalties on IOM companies? Could an IOM firm still be subject to 4% / £20m fine even if IoM max penalty is set at £1m?	• Further reading: ○ Article 29 Working Party – Guidelines for identifying a controller or processor's lead supervisory authority – http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf ○ Article 29 Working Party – Guidelines on the application and setting of administrative fines - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 ○ ICO Isle of Man - May 2017 conference responses – question category on Supervisory Authorities and representatives, and Enforcement and penalties: https://www.inforights.im/media/1379/gdpr-conference-slido-reposnses_may2017.pdf Note: the Article 29 Working Party will become the European Data Protection Board in May 2018. The guidance issued is applicable to all Member States, which for the purposes of the applied GDPR (being the GPDR as applied to the Isle of Man by order, with the adaptations set out in that order), will include the Isle of Man. The guidance sets out standards and requirements that should be followed.
Compliance/Readiness - Given the new powers of the Information Commission, will there be a more proactive review to Compliance with GDPR, for example onsite reviews? - How will the ICO police GDPR? - If data is put beyond use is that acceptable as an interim measure for companies while	The tasks of the IC include to monitor and enforce compliance. This will mean that the IC will take a more proactive review of compliance including onsite review. The IC will continue to investigate complaints, initially proactive monitoring is likely to take two forms: an examination of a controller's website where applicable and compliance questionnaires. Other monitoring may occur subject to risk assessment. Putting data beyond use may be acceptable, subject to risk to a data subject, where a controller or processor is able to evidence that they are actively taking action to achieve compliance. Data Protection policies are not new and existing guidance exists. For example: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/ It depends on the risk posed by the nature of processing as to the need for data protection policies. Article 24

working towards compliance? - Will there be guidance on drafting data protection policies. Where will this be held? Is it a requirement that all companies have a data protection policy by May 18	of the GDPR requires controllers to implement appropriate data protection policies that are proportionate to the severity and likelihood of risk to an individual.
Requirements for Data Protection Officers - Do we need a data protection officer (internal or external) even if we are a very small company - less than 20 people - GDPR only requires a DPO to be appointed in certain circumstances. Are you implying that all IOM processors will have to appoint a DPO? - How is large scale of processing data defined? - For companies that are multi-jurisdictional, ie cover CI & IOM. Will the IOM operation require a Data Protection Officer, or can one person cover all three	• Article 37 of the GDPR requires the designation of a (DPO) for: o Processing carried out by a public authority or body o Processing operations which require regular and systematic monitoring of data subject on a large scale or o Core activities consist of processing on a large scale of special categories of personal data. • Article 37 does not otherwise require designation of a DPO. However, there may be certain organisations which determine that a designation of a DPO is necessary, taking into account the organisational structure and size, and the level of processing and nature of the core activities (even if they do not fall into a category above) together with the level of risk. • It is difficult to set out guidance for DPOs within set parameters for example the number of employees – since a small corporate service provider with 5 employees may process significantly more personal data (or sensitive personal data) than a freight company which employs 500 people. • 'Large scale' processing is not defined in the GDPR. The Article 29 Working Party guidance on the topic sets out certain examples of what might be considered large scale processing, which take into account the number of data subjects, the volume of data being processed, duration/permanence of processing activity, and geographical extent of the processing activity. • For companies which have more than one office (wherever situate), guidance says that one DPO could cover all offices, but again this is dependent on the nature of processing, size and structure of the organisation. The location of the DPO will depend on where the DPO can carry out his or her duties most effectively. • A DPO can be appointed by a service contract and need not be an individual, the DPO can be a corporate entity. • A DPO should have sufficient independence in their duties, but in accordance with the tasks and duties imposed upon them by the GDPR, they also require to have access to the highest level of governance for the organisation, so in most cases board or senior management team level. The practical requirements for meeting attendances, reports or otherwise will again depend on the nature of the processing, the structure and size of the organisation and its requirements.

islands? - Can a DPO be a corporate? - Will there be a local expectation on the minimum qualifications for DPOs? - If you have an external DPO, how integrated into the business do they need to be? Should they attend board meetings, management meetings on a regular basis - What are DPO minimum qualifications required? Are there IC approved providers for IOM DPOs? - How do we find out about the local GDPR/Data Protection Officer forum? - If you have a trade union member on your payroll, or onsite CCTV, does that require that we have a DPO? - If a company undertakes regular monitoring of all its clients for AML risk	• A DPO does not require a specific qualification and at the present time there are no certified qualifications in GDPR but there are a number of certified and endorsed courses in the United Kingdom carried out by various providers. • There are no plans by the Isle of Man Government to provide training at a local level to DPOs in the private sector, outside of general guidance. • There are various on Island shorter courses for GDPR compliance which are available, but training requirements may differ by organisation. • There is a local DPO Forum which is run by representatives from SMP Partners, PWC and Appleby, with other co-opted committee members. A LinkedIn group is available to join and contact details can be obtained from the Information Commissioner's Office. • Further reading o Article 29 Working Party - Guidelines on Data Protection Officers - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 o Isle of Man Information Commissioner – 'A Closer Look at Data Protection Officer' guide - https://www.inforights.im/media/1416/dpo.pdf o https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

assessments but has less than 500 clients would this been seen as requiring a DPO ? - Given the deadline, is there a locally based intensive DPO training course?	
Legislation - If the forthcoming Bill is to enable the EU regulations to be brought in to Manx law, how can you make amendments to them as a result of the consultation? - Modifications and exemptions: with no trust law revision, will there be consideration to allow access of beneficiary information to trustees in order to maintain the trust? - Why has it taken so long to get the draft legislation? - Will you provide a gap analysis between existing and new legislation? - Why are we retaining a notification requirement? - Is it proposed to extend regulations	• The draft legislation has been drafted following analysis of approaches by other jursidictions, in order to produce a bespoke product for the Isle of Man. Whilst in the UK and Channel Islands, legislation was published earlier, in each of Jersey and the UK, it is only just going through final approval/Royal assent stages now. With the intention to shorten the legislative process for the Bill with a truncated process, the Isle of Man intends to hit the same deadline with its proposal for its new Data Protection Bill. • The proposed Bill replicates powers which already exist in the European Communities (Isle of Man) Act 1973 (the 1973 Act), and consists of 7 clauses. The 7 clauses of the Bill essentially set out the power for the Isle of Man to implement any EU Instrument relating to data protection, by order in Council. • The Bill, if passed, will permit the GDPR and LED to be implemented into Manx domestic law by order in Council (the Orders). This will constitute the primary legislation and shall be entitled 'the Data Protection Act 2018'. • The Orders will respectively annex a copy of the GDPR and LED, with local modifications and adaptations (i.e. where the GDPR says 'according to Member State law', it might read 'according to Manx law', and the annexes will delete provisions which are only relevant in an EU context rather than to read as domestic law). • The powers granted by the Bill will allow implementing regulations to be made. The implementing regulations contain the substantive provisions for data protection, which include some of the current provisions of the Data Protection Act 2002, and give more detail as required by the GDPR and the LED, taking inspiration from various other jurisdictions. • For example, the retention of the notification process to the ICO (as set out in the existing Data Protection Act 2002 at sections 13-17, brings with it consistency and a clear mechanism by which we can add the GDPR requirement for organisations to notify the ICO of the identity of their DPO. We consider that this is another step towards accountability and demonstrating compliance as required by Article 5(2) of the GDPR. We invite views on this and any other mechanisms that are considered necessary (or unnecessary as the case may be) in the consultation. • During the consultation process, we would be interested to hear views specifically on required modifications and/or exemptions which may be required, for example for trusts to permit access to beneficiary information (as it is acknowledged that the beneficiary may not have specifically consented to the information processing). The project team will then consider any necessary consequential amendments in other legislation (such as trust law, Freedom of Information, AML legislation and

beyond EU to worldwide? - Schedule 10 of the Regulationss specifically excludes public authorities from some exemptions, including where explicit consent already exists - why? - Will there be amendments to the AML legislation/ guidance on retention of records of individuals who have been subject to a SAR? Are the FIU engaged?	guidance, and various other public sector guidance, safeguarding or otherwise). • The term 'regulations' in this context means the implementing regulations, which give the power to implement the processes of the GDPR and the LED into Manx domestic law. • The Isle of Man Government, including all of its Departments, Offices and Statutory Boards have been fully engaged in the pre-consultation process by way of briefings to Senior Management Teams and Boards, and Data Protection Officers now appointed across Government liaising with those Senior Management Teams. • A specific exclusion for public authorities from some conditions of processing is included in the draft regulations because the first principle of the GDPR (lawfulness of processing), is qualified by the conditions set out in Article 6(1)(e) of the GDPR, which provides that one of the lawful reasons for processing personal data is met if the processing is necessary for the performance of a task in the public interest or in exercise of the controller's official authority. • Consultation on the implementing regulations will afford all stakeholders an opportunity to be involved in shaping the future of data protection law in the Isle of Man. • The Isle of Man has committed to introducing essentially equivalent legislation that maintains the adequacy finding from the EU and is in direct contact with the European Commission in relation to its intended approach and the legislative process. **Further reading:** • Consult.gov.im – online consultation - https://consult.gov.im/cabinet-office/new-data-protection-bill/
Adequacy - Will adequacy status remove the need under EU GDPR for a Manx controller selling into the EU to have a nominated representative locally in the EU? - Are there any risks that our legislation will not gain equivalence status should we diverge, albeit subtlety, from the international Standard.	• Adequacy does not avoid the need to comply with the provisions of the GDPR. • The adequacy finding is based upon the existing provisions of the Data Protection Act 2002, and the Isle of Man Government is satisfied that the proposed mechanism by which it intends to directly import the provisions of both the GDPR and LED will meet the requirements for adequacy. • The Article 29 Working Party guidance on the adequacy referential sets out specifically that there is no requirement to mirror legislation point by point, but that essentially equivalent legislation should be in place. • The Isle of Man's proposed mechanism is a bespoke solution for the Isle of Man since we are a third country and not a member state of the EU. • The Isle of Man has a very different starting point than other jurisdictions, and the proposed approach is a more direct one, to import the text of the GDPR and LED into our domestic law (with some local modifications). Other jurisdictions have chosen to implement 'essentially equivalent' legislation intended to look like the GDPR and LED in practice. • As to modifications and adaptations locally, the only deviations from the GDPR and LED will be those which are permitted by its provisions. • By way of example in respect of 'local' deviations from the provisions of the GDPR: o administrative fines under Article 83, permit provision for administrative fines **up to** certain

- Once the IOM regulation is finalised, is there a risk that the EU will not deem it as Adequate?	levels, but do not **require** jurisdictions to implement the maximum penalty. o in relation to children's age of consent for information society services in Article 8, the GDPR permits jurisdictions to select a lower age provided that such age is not lower than 13 years. • In assessing adequacy, the Commission would consider the rule of law, respect for human rights and fundamental freedoms, the relevant legislation, the existence and effective functioning of the supervisory authority (in our case the ICO), and any other international commitments and relationships. In other words, it will consider the legal rules applicable in any given jurisdiction and the means for ensuring their effective application. Further reading: • Article 29 Working Party Guidance – Adequacy referential: ec.europa.eu/newsroom/just/document.cfm?doc_id=48827
Advice, Guidance and Resources	
- Interpreting the definition of a "legal person" how would this impact on the scope of "personal data" that is being processed e.g. processing on multiple companies? - Does data include handwritten information and hard copy files and notes or purely electronic information? - As an extension of the legal entity - are we right to assume that irrespective of where a branch is located that they are in scope for IOM GDPR or exempt?	• The GDPR contains a number of definitions which are intended to be qualified by the proposed draft regulations. See the ICO's further guidance in respect of definitions in the GDPR here: https://www.inforights.im/media/1408/definitions.pdf • The definition of data often depends on the circumstances. "Data" includes automated personal data and manual filing systems, so it may include handwritten information and hard copy files since they may fall into the these categories, (or for an FOI public authority) to which the GDPR applies. The current definition of personal data has been extended by the GDPR and now means: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" Art. 4(1) (Definitions) Rec. 14, 26-30 • Territorial scope of the GDPR includes processing within the EU and processing of EU citizens data. The GDPR does not allow forum shopping, and irrespective of where a branch is located, depending on processing activities it may be caught within the scope of the GDPR as applied to the Isle of Man (described in the draft regulations as 'the applied GDPR') • There are some questions and answers for charitable organisations in relation to the GDPR here: https://ico.org.uk/for-organisations/charity/charities-faqs/ As currently drafted, the IC is required to consult with Council of Ministers, trade associations , data subjects and others before preparing such a codes. As such codes already exist in the UK and similar codes are required than they are likely to be based on the UK codes. Any feedback on whether the codes should be introduced in the Isle of Man's legislation at all is welcome at http://consult.gov.im .

- Could you please give more info for information holding for small community organisations such as a local camera club? - When will we get the codes from the ICO referred to in the regulations? Noting businesses must be compliant by 25 May and introducing new T&Cs etc takes time - Does GDPR have a requirement for data to be stored in a certain country? - Is there a PIA template available from the ICO? - If someone gave you a business card in 2016 does that meet consent criteria or do you need to contact them to get updated consent? If so how often? - What is the IC's view on historic data systems where data cannot be deleted or obscured or it is too expensive to do so? Will a written plan be sufficient? - Is there a pool of	UK Codes of practice: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf https://dma.org.uk/article/the-new-statutory-direct-marketing-code-of-practice • The ICO in the UK has set out specific guidance for small organisations which can be found here: https://ico.org.uk/for-organisations/business/ In addition, there are a number of resources on the Information Commissioner (Isle of Man) website at www.inforights.im, including a '10 things you need to know and do', essentially a 'beginners guide' to the GDPR: https://www.inforights.im/media/1383/10things_may17.pdf • The Irish DPC has also produced a checklist for SMEs: http://gdprandyou.ie/wp-content/uploads/2017/12/A-Guide-to-help-SMEs-Prepare-for-the-GDPR.pdf • There is no requirement for data to be stored in a certain country. However similar to current legislation personal data must not be transferred to another country outside the EEA unless that data is adequately protected. Under the GDPR controller and processors must be able to demonstrate and evidence that the personal data is adequately protected. • Privacy Impact Assessments have existed as good practice for some time. The EU Art 29 Working Party which becomes the European Data Protection Board under the GDPR has published its guidance on PIA's which can be found at: file:///C:/Users/odpsimac/Downloads/20171013_wp248_rev01_enpdf%20(2).pdf see also http://www.piafproject.eu/ref/PIAF_D3_final.pdf The UK ICO also has a PIA code of practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf • A controller in the private sector does not need to rely upon consent to contact someone who has provided that controller with a business card. Instead that controller can reply on legitimate interests lawful processing provided the purpose for which the controller intends to process the personal data on the business card is compatible with the purpose for which it was given then there is no need to contact. However if the data subject subsequently contacts the controller and objects to that processing then the controller must comply with that right. • If it is not currently possible for a data controller to delete data when it is no longer necessary , then the controller by keeping data longer than necessary is likely to be contravening the current fifth data protection principle. A controller must be able to delete such data. • If a controller does not delete personal data due to the cost of doing so then the controller should expect to receive a penalty that is greater than the cost of deletion. It is also important to appreciate that if data is not deleted then all the data subject's right including the right of access and the right to object to processing will continue to apply. • At the moment there is no information as to how many organisations/people hold the BS10012 (the British Standard for data protection) in the Island. It is unlikely that Government would convene such a

bs10012 internal and external auditors. If not, is it reasonable to convene one for the benefit of all of us as an island? - The positive impacts of the GDPR seem solely for larger businesses and internationally. What positive impacts do the panel foresee for smaller local businesses?	pool, but the private sector may wish to do so. • Small and indeed some of the small to medium enterprises may well find the provisions of the GDPR burdensome upon its operational mechanisms. However, good information security and governance still makes good business sense and contributes to the wider business and local economy in the Isle of Man. As a small business, good governance in the area of GDPR and data protection will improve perception and reputation of that small business, and increase consumer confidence. The spirit and intention of GDPR is to create a culture of protection of data and data subjects rights and ensuring compliance.

Definitions:

WP29 - Article 29 Working Party (to become the European Data Protection Board in May 2018)
GDPR – General Data Protection Regulation
LED – Law Enforcement Directive
ICO – Information Commissioner (Isle of Man, unless otherwise stated)

Disclaimer: The responses contained in this document are intended to reflect the broad requirements of GDPR and the LED, and the legislative mechanism by which it is intended to introduce those provisions into the domestic law of the Isle of Man. The responses contained do not constitute legal advice and should not be relied upon, or distributed in any form without written permission from the Cabinet Office. It is strongly recommended that organisations take their own legal advice in relation to any specific legal issues. Guidance and other references are included in the responses as suggestions for further reading, but other resources are available.