GDPR Conference 10 May 2017
Sli.do question responses

information commissioner
Barrantagh Fysseree

Responses to Sli.do questions not answered during panel sessions

The questions received have been grouped into themes. In most cases the answers can be found in the GDPR Articles and Recitals or on our website or in other resources. References are made accordingly.

Link to the GDPR:

http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1462369452037&uri=CELEX:32016R0679

The following acronyms are used in the responses:

"Art" = Article of the GDPR
"Rec" = Recital of the GDPR
"IC" = Isle of Man Information Commissioner
"UKIC" = UK Information Commissioner
"EDPB" = European Data Protection Board
"WP29" = Article 29 Working Party

Question Categories are:

- Definitions
- Consent
- Isle of Man Law and Guidance
- Territorial Scope
- Data Protection Officers
- Data Breaches
- Data Minimisation
- Supervisory Authorities & Representatives
- Security & Data protection impact assessments
- Fines and other penalties
- Rights
- Uncategorised

NOTE: The responses provided do not constitute legal advice

Question Category: Definitions	Response
What will constitute personal data?	The current definition of personal data has been extended 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 https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/gdpr-in-depth/definitions/
Please define a "European Person" - Residency, nationality? EU person includes nationals outside of EU & any EU residents regardless of nationality even if you don't market to them?	Art. 3 Territorial scope (in particular Art. 3(2)) Rec. 22-25 "data subjects who are **in** the Union" - i.e. it applies to individuals resident in the EU, irrespective of nationality, but not to EU nationals who are not resident in the EU. https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/gdpr-in-the-island/why-are-island-businesses-affected/
What are the panelists' general views in respect of GDPR and insolvency cases, i.e. the duties of the liquidator and or trustee in bankruptcy?	Needs assessment on a case-by-case basis: Is the entity a data controller? – what does the insolvency legislation state about the role and function of liquidators or trustees in bankruptcy and do those functions include the processing of any personal data? What (if any) personal data is processed? Are any data subjects resident "in the Union"? Does the processing of personal data of data subjects in the EU fall within the descriptions in Art. 3(2) and engage the GDPR?

Question Category: Consent	Response
At what age would Parental Responsibility over ride a child's consent not to disclose information relating to the child to the parent?	The only reference to the age of a child in the context of consent is in connection with **information society services** (e.g. use of social media website) Art. 8 Rec. 38 This age specification does not apply to the exercise of any rights including the right of access, or impact on consideration of disclosures of personal data to third parties (including parents). Art 40 (f) – Codes of Conduct also refer to obtaining children's consent.

Question Category: Isle of Man Law and Guidance	Response
When should we expect the new draft data protection bill For Ian; is there a timetable for the release of the new isle of man legislation & guidance?	The Chief Minister has committed to implementing essentially equivalent legislation by May 2018. The timetable is dependent upon drafting availability and production in the UK of draft legislation. It is a matter for IOM government and the Attorney General's Chambers legislative drafters and is not in the hands of the IC, although it is recognised as being extremely tight.
When is the ICO GDPR Guidance (as referenced) expected to be finalised / published?	Advice, as far as it is possible to provide it, is available on the IC's website by following the link to the GDPR section from the home page: https://www.inforights.im/ Some of the UKIC guidance and codes of practice referenced during the day are on the memory card supplied – other guidance is available on its website www.ico.org.uk and via its dedicated area, "Data protection reform (GDPR)" If you provide goods or service to EU residents you need to look at the guidance issued by the WP29/ EDPB and the relevant lead supervisory authority.

Question Category: Territorial scope	Response
How will non EU companies even know they have to comply with gdpr if serving EU citizens, let alone be enforceable?	It is the responsibility of the Directors and officers of the company to ensure that they understand what laws apply to it. Achievement of trans-jurisdictional enforcement is a matter for the EDPB. However, there are already global enforcement networks, including the Global Privacy Enforcement Network (GPEN), of which the Isle of Man Commissioner is a member, which assist in such matters.
Is one happy result of the gdpr is the enabling of archaic + less effective EU providers as a non-tariff barrier? What happens to the US internet giants?	Whilst we are not quite sure what the first part of the question is about, the answer to the second part is that "US internet giants" that fall within the scope of the GDPR must comply with it. To that end, several major companies (e.g. Microsoft, Facebook, Google) already have operational bases in the EU and accept that they are subject to the GDPR. Companies based in the US and subject to the GDPR may also sign up to the voluntary Privacy Shield operated by the US Department of Commerce - https://www.commerce.gov/tags/eu-us-privacy-shield
If someone bought a policy years ago in a non EU country but subsequently moves to live in an EU country are they caught?	At the moment this depends on the answer to the question as to whether the territorial scope of Article 3 applies to the processing i.e. offering goods or services to persons etc. in the Union. In the longer term, as the Island has committed to implementing "essentially equivalent" legislation to the GDPR, the need to consider the physical location of data subjects is likely to become unnecessary as the Island's legislation will be likely to apply to all personal data being processed irrespective of their location.

Question Category: **Data Protection Officers**	**Response**
Various questions were asked about • the appropriateness of a person to be a DPO, • the 'qualification' requirement • the possibility of further guidance	Guidance on the appropriate person to be a DPO ("conflict of interest") and on their 'qualification' (or "expertise and skill") has been adopted by the WP29. WP29 will become the EDPB in May 2018. Guidance issued by WP29 and EPBD is applicable across Member States. These are the standards and requirements that need to be followed. Challenges to the interpretation of the GDPR in EDPB guidance can be made to the EU Court of Justice. Guidance on DPOs was adopted by Art 29 WP in April: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 "conflict of interest" - section 3.5 "expertise and skill" – section 2.5 Art. 37 - 39 Rec. 97
The IOM Info Commissioner has intimated that financial services business will be obliged to appoint a DPO regardless of processing activities. Pls confirm	Where the processing amounts to *"regular and systematic monitoring"*, a DPO will be required. Para. 2.1.4 of the Article 29 document covers this aspect and specifically includes: *"profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering)"* Businesses undertaking KYC/CDD checks will be undertaking "regular and systematic monitoring" and therefore appear to require a DPO.

Question Category: Data Breaches	Response
Will the IOM ICO give guidance on materiality for data breaches that need to be reported?	Guidance will be issued by the EDPB in due course. That guidance will inform any advice issued by the IC and all other EU data protection authorities. Articles 32-34 Recitals 39, 49, 74-77, 83-94
Would putting a valuation for a client into another client's envelope be a breach? It would include name, address and statement of value of their policy.	A disclosure of personal data to a third party would occur, which may result in a risk to the individual. Would need to consider whether a breach report was mandatory, and if so, to whom. Considerations could include the security measures in place and whether they were followed; the effect of the disclosure on individuals. (Good business practice would be to manage the client trust issue by communicating with the client and protecting their interests even if it a report is not mandatory) See Art. & Rec. above

Question Category: Data Minimisation	Response
I see a real tension between customer due diligence where the regulator thinks you should have as much information as possible and data minimisation - agree?	Art. 5(c) Rec.41, 45, 47 Personal data shall be: (c) adequate, relevant and **limited to what is necessary in relation to the purposes for which they are processed** ('data minimisation'); Chapter 5 of the new AML4 refers explicitly to compliance with the existing EU Data Protection Directive 95/46/EC including the "necessary documentation" (by reference to Chapter 2 of AML4, Customer due diligence), retention periods, the issue of fair processing information, and states that processing is only for AML obligations and no other commercial purpose (e.g. marketing). What is "necessary" in the context of due diligence will be informed by the legal landscape being applied by the regulator. Any information over and above that mandated in law will (as currently) be unlikely to be "necessary" for the purpose.

Question Category: Supervisory Authorities & representatives	Response
Will lead supervisory authorities only apply for organisations established in the EU? When would an IOM company need to appoint a LSA if it has no EU presence? Will all third country data controllers require a presence/ agent within the eu and how is this likely to work practically? How do regulators co-ordinate complaints? A Manx Co contracts with an English Co to send out marketing emails to people in Germany who complain it's unsolicited**	A **Supervisory Authority** is one of the EU Member State data protection regulators. Any organisation outside the EU falling within the scope of the GDPR will need to identify which EU member state the individuals, who are the main target of its marketing, services or profiling, reside in. An IoM company may need to identify which is the data protection regulator in the most relevant Member State. A **'lead supervisory authority'** is the authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of their personal data. Identifying the lead supervisory authority is covered in the Annex of the WP29 guidance below. Data controllers subject to the GDPR may need to appoint a **representative** in an EU member state. Art 27 & Rec 80 – representative Art 55-59 & Rec 122-129 –Independent supervisory authorities Art 60-62 & Rec 130-134– co-operation, mutual assistance and joint operations of supervisory authorities WP29 adopted guidance on **Lead Supervisory Authorities** http://ec.europa.eu/newsroom/document.cfm?doc_id=44102 IC website link https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/gdpr-in-the-island/representative-lead-supervisory-authority/ ** (**Note:** the example of complaints about unsolicited direct marketing emails falls within the E-Privacy legislation – although the responsibility for compliance with that legislation may sit with the same regulator as the data protection legislation. **See also** the response in the 'Uncategorised' section regarding the proposed changes to the E-Privacy legislation)

Question Category: Security & DPIAs	Response
When using the cloud do we have to know 'where' it is and if this is gdpr compliant?	Yes, controllers are responsible for the personal data of their clients and must know where that personal data is located. This is also the current position. Cloud service providers will act as data processors and servers may be located in one, or more, or variable, jurisdictions which may not be in the EU, the IoM, or any other adequate jurisdiction. Controller engaging processors are required to ensure that the processor guarantees that the personal data is adequately protected and ensures the protection of the rights of the data subjects. Art 24-29 & Rec 74-81
What is the position under the GDPR if I use my phone / tablet to access data held by my company when overseas (non-EU)? What safeguards could we put in place?	The data controller must ensure that appropriate security measures are in place, irrespective of where in the world personal data is accessed from. Safeguards will be dependent upon the nature of the personal data and the processing that is being undertaken. Security measures should be designed in and be subject to regular testing and form part of the records of processing activity. Art 32 & Rec 39, 49, 74 – 77, 83-94 – security of processing Art 24,25 & Rec 74-84 – responsibility of controllers and data protection by design and default Art 30 & Rec 82 – records of processing activities
To what extent should we be carrying out retrospective PIAs for higher risk processing activities, if we haven't already done one?	Data Protection Impact Assessments (DPIAs) should be carried out prior to processing. There is no express provision in the GDPR for post-implementation DPIAs. However, the security element of any processing should be subject to regular review and should there be a change in the type of processing, the risk to data subjects etc, then a DPIA may be considered on the basis of the changes.

	In practical terms a DPIA will help businesses to identify whether the security of personal data, in particular, is appropriate. WP29 is currently consulting on its DPIA guidance (ends 23 May 2017) http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 The UKIC has a code of practice on conducting Privacy Impact Assessments that provides guidance in the meantime. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
What is the crossover between the FSA given their cyber security guidance and the standards which the ICO expects?	The GDPR (and the existing DPA) applies only to information which is personal data. The security measures, required records of those measures and evidence of the testing of those measures, are legal obligations in respect of personal data. The guidance issued by the FSA regarding cyber security standards applies to all forms of information and is not limited to personal data. Whilst applying to personal data as a form of information, regulatory guidance does not have the force of law in respect of the protection of personal data.

Question Category: Fines & other penalties	Response
How is global turnover calculated when applying penalties? How are the fines structured (both tiers)... just company/authority or personal director/CEO too? How will derogations impact this position? Is there a right of appeal over fines imposed?	Supervisory Authorities have various powers set out in Art. 58 (& Rec 122, 123, 129), which include imposing administrative penalties (fines), issuing warnings and reprimands and, as identified in the Conference, probably the most significant being the imposition of a processing ban. Details about the fine regime (which may be imposed in addition to other measures) including the basis for the calculation of global turnover are in Art. 83 and Rec. 147, 148, 150, 151 The criteria for the fine calculations have still to be determined. Fines imposed by EU supervisory authorities will be payable to them. Art 83(8) & Rec 148 – refers to the right of appeal Art 84 & Rec 149 - Other "effective, proportionate and dissuasive" penalties, including personal criminal sanctions, must also be implemented in the domestic law of Member States.
Highest profile breaches have been by government departments. How will ICO deal with government breaches, will fines be imposed and where will the fines go	Fines may be imposed on public bodies – this decision must be determined by each Member State. Art 83(7) Rec 150 However, where no provision is made for the imposition of administrative fines on public bodies, Art. 84 requires that alternative penalties which are "effective, proportionate and dissuasive", including personal criminal sanctions, must be implemented. These penalties can be imposed on a public body and its officers. Fines imposed by the IC under equivalent legislation implemented in the Island are likely to be paid into Treasury general revenue.
What should we expect in terms of enforcement from the IOM ICO?	This depends on what the new legislation in the Island looks like. It should be "essentially equivalent", so the powers and sanctions should not be dissimilar. The role of the IC will change from a duty to 'promote observance of the requirements of the Act' to "monitor and enforce compliance with" any new Act. Data controllers can expect their processing to be monitored and audited for compliance.

Question Category: Rights	Response
Could you explain more about **portability**. Why would a company be obliged to transfer or provide usage data?. Is that deemed to be personal data?	Art. 20 Rec. 68 The WP29 has adopted guidelines on this topic which can be found: http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 The definition of personal data can be found in Art 4(1) Rec 14, 26-30
What impact to you see (if any) GDPR having on FATCA/CRS? For example what if a client requests to be **forgotten**?	Art 16(2) &17 & Rec 65,66 Right to be forgotten (the right to erasure) is not new and is not unrestricted and only applies where processing infringes Art. 4 (principles), 8 (lawfulness) or 10 (special categories) (or if the controller is subject to a legal obligation requiring erasure, such as a court order). If the processing is lawful, complies with the principles etc. it is unlikely that a request to erase that personal data will need to be complied with. Case by case analysis will be required.
When provided information in confidence about another third party , would this trump disclosure in regards to a **subject access request**	This is not the case now under DPA and is unlikely to be affected by GDPR. Section 23(5) of the DPA 2002: *"Except as provided by this Part [Part 4 – exemptions], the subject information provisions shall have effect notwithstanding any statutory provision or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information."* Confidential personal data relating to the data subject can only be withheld from disclosure under the right of access if an exemption from that right set out in Part 4 of the DPA can be relied on.
How can anyone be given the right to sue for **damages** without having to prove they've suffered any loss?	Art 82 & Rec 146, 147 This is a standard judicial remedy for *"material or non-material damage"* Both controllers and processors may be liable but are exempt from liability *"if it proves that it is not in any way responsible for the event giving rise to the damage"* A direct approach for compensation to a controller or processor is not precluded.

Question Category: Uncategorised	Response
Will this not have the effect of pushing online organizations into jurisdictions which are non-cooperative with the GDPR (ie refuse to cooperate)?	'Co-operation' applies to the engagement between supervisory authorities. The choice of jurisdiction is a business decision. Businesses should consider the trust, and expectations, of their customers in the use of their personal data and their ability to exercise their rights. Equivalent legislation exists in many countries, for example APEC (Asia Pacific Economic Cooperation) already has cross-border privacy regulations. http://publications.apec.org/publication-detail.php?pub_id=390
Is there a conflict with mifid 2 in terms of transaction reporting where information will be shared with eu each time a trade is undertaken in financial markets	There is unlikely to be a conflict if the processing and disclosures of personal data are mandated by law and accord with the principles (noting that this applies only to the personal data element).
How far can a business rely on publishing privacy notices on their website	Privacy notices form part of the transparency requirements and must be found easily, and be in clear and plain language. Art 13 & 14 & Rec 39, 58-62 There is no definitive answer to that particular question in the GDPR. Rec 57 states *"Such information could be provided in electronic form, for example, when addressed to the public through a website"*. This must be a common sense approach - Is the only interface with individuals via a website? How do you tell them that the privacy notice is on the website? What if people do not have access to the website? How much do you tell them initially? What if they want to know more detail? The UKIC's Code of Practice on Privacy Notices provides helpful guidance and is on the memory card.

Do organisations have a responsibility to confirm third party suppliers are GDPR compliant?	This is taken to refer to the use of third party direct marketing list suppliers. The business responsible for sending (or instigating the sending) of direct marketing must ensure that consent to marketing from the sender has been obtained and can be evidenced. This is likely to impact, in particular, on affiliate marketing practices and the trade in lists of email and mobile numbers of individuals that have purportedly 'consented' to receive direct marketing. A full understanding of the definition of consent is required and the changes to the e-Privacy Directive should be noted (see below for links to the e-Privacy Directive changes) Guidance on direct marketing is available on the website: https://www.inforights.im/information-centre/direct-marketing/guidance-for-marketers/
Will it be acceptable to collect info via cookies and use that to market via pop-up in other sites?	The existing e-Privacy Directive, which applies to electronic direct marketing and includes the use of cookies, is currently being reviewed and will take the form of an EU Regulation rather than a Directive. In the current draft Regulation, cookies are likely to be **opt-in** to accord with the definition of consent within the GDPR which is imported into the draft e-Privacy Regulation. Details on the progression of the e-Privacy Regulation can be found at: https://ec.europa.eu/digital-single-market/en/online-privacy
The uk is consulting on derogations, should there be any derogations, what is the panels view on what impact may be on equivalency ratings	Minimum standards must be maintained, but the application of derogations is a political decision for UK government. The Island is committed to introducing essentially equivalent legislation that maintains its adequacy finding from the EU and will enter into direct dialogue with the EU regarding the adequacy of the new legislation.
How will all of this apply to small businesses such as a beautician/spa that could hold health data? Will the IC be	Unless the small business targets customers who are "in the Union" the GDPR will not directly apply. However, the changes to the IOM legislation will be likely to bring about will affect all controllers and processors in the Island.

presenting to small businesses?	The IC has, and will continue, to produce advice and give presentations to trade/industry associations on GDPR.
Seems like the IOM IC will have a lot more work on its plate... how will it do this with its current resource? Doesn't it only have a handful of staff?!?	Yes, it is anticipated that there will be increased pressure on the current 4 members of staff. Increased staffing and funding are likely to be required and this will be a matter for negotiation by the IC. However, as an alternative approach, the IC may consider seeking the assistance of the private sector in auditing the compliance of data controllers. Articles 51-52 of the GDPR require supervisory authorities to be: • completely independent • remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody, • is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers • is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.