IOB World Data Protection Day event 28 January 2021

Participant Questions

1.	Can DPC issue guidance regarding processing data for AML/CTF purposes
	Through our work with the European Data Protection Board (EDPB), we are currently organising a research project on GDPR compliance when doing AML collection and processing. Once this research project is finished then there may be a follow up guidance document that could issue from the EDPB to ensure that there is a consistent approach across all Member States. In the meantime please see attached link with observations to the CBI https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp128/data-protection-commission-response-to-cp128.pdf?sfvrsn=3
2.	Hi Garrett, A Credit Union may have some indication that their software provider (data processor) has been uploading inaccurate data to the CCR. The matter has been raised with the sub-processor and a breach report submitted DPC. Rectification of the software seems complex and the data processor has indicated that they are working with the Central Bank to rectify the matter. When is it envisaged that the new procedures to update the CCR are put in place?
	From our engagement with CBI, the CCR team are constantly attempting to resolve any problems or issues with uploading data to the CCR and have produced guidance notes to that effect. This is an issue that needs to be dealt with directly with the CCR team in CBI.
3.	For insurance companies, where quotes are obtained, should they delete the information straight after also, as each year some companies would contact as they have kept the information on file, whereby I would have to unsubscribe (even though I never opt in for communications).
	Any sector that is providing a quotation service, which collects personal data from individuals, should be reviewing its retention policy as to why it is necessary to retain any or all of the data collected, especially where the customer does not proceed to enter into a contractual arrangement. Any regulatory requirement such as the CPC by CBI must balanced with the Individuals right to exercise an objection to such retention or a right to be forgotten i.e. the individual is not pursuing any other regulatory remedies. The retention

of such data must be lawful fair and transparent to the individual. If the data controller is retaining this data under a "Legitimate Interest", then a DPIA needs to be done that properly assesses the risks and balances the rights of the Individual to those of the DC. I assume that any consumer that wished to make a complaint about an unfair quotation would keep the quote as evidence, should they decide to contact the financial ombudsman or other regulator. It is not for the service provider to prove that a quote was unfair based on the facts it had, to assess the individual. What it does have to show is that its processes are fair, in making the assessment. If a person is refused a quote or a service then reasons should be given as to why this has happened.
If any sector is interested, the DPC will assist in the development of a Code of Conduct on this issue.

4. Hi. what happens when AML objectives take precedence at the expense of data protection obligations? how can we apply the correct data protection principles while still meeting the AMl objectives? One law does not take precedence over the other. Both have to be complied with.
One of the key elements in the 4th Directive is for Data protection rules to apply in any implementation of AML.
This is set out in the 4th AML Directive 2015/849 in Recital 43, which states …
It is essential that the alignment of this Directive with the revised FATF Recommendations is carried out in full compliance with Union law, in particular as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter. Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data. Such processing of personal data should be permitted, while fully respecting fundamental rights, only for the purposes laid down in this Directive, and for the activities required under this Directive such as carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities. The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the requirements of this Directive and personal data should not be further processed in a way that is

incompatible with that purpose. In particular, further processing of personal data for commercial purposes should be strictly prohibited.
5. Interested in Garret's view on phishing. Where the customer has provided their codes to the fraudsters who use that information. The financial services firm has not been involved in the phishing - it has not disclosed any information. In that case what is the breach that a financial services firm has to report, where the disclosure was by the data subject
If the Phishing attempt resulted in an unauthorised access to the customers A/c or information held by the DC then it is a security breach that has to be reported to the DPC and the Individual so that s/he can change their passwords or codes.
6. is there official guidance from DPO on the reporting of phishing and smishing incidents etc? how, when, what etc. https://www.dataprotection.ie/en/dpc-guidance/guidance-organisations-phishing-and-social-engineering-attacks
7. justification to keep data just in case of legal proceedings / complaints, surely that could be applied to all data - thought that expectation of legal cases / complaints was not a reason to keep data
Retention of any personal data has to be properly justified as a necessary requirement. The "Just in Case", reason for keeping the data is not a good explanation. That is why Data Controllers really need to think as to why they are retaining any data and what problems it could cause them if they delete it or retain it. What the DPC is looking for, is a proper explanation as to why the data has been retained or deleted. I would recommend that a DPIA is done to assess this problem within the organisation. Article 5.1 (e) of GDPR applies... ***kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the***

	appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
8.	CCR- are the Dpc expecting organizations to reporting breaches of accuracy principle to the DPC via personal data breach channel.
	That is not a security breach. But it is an infringement of GDPR if the DC has inaccurate data on it's customers. It is a legislative requirement in the public interest, for the DC to disclose credit data of its customers to the CCR. The data disclosed must be accurate or else it will probably cause a harm or detriment to occur to that customer, if that person seeks future credit facilities from any third party credit provider and is refused or given higher interest rates etcetera because of the inaccurate data on the CCR. Art 5 .1 (d) of GDPR applies... ***accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');***
9.	Why do the speakers believe the AML practioners hold AML requirements override DP requirements? Have been told this on several occassions also on training courses.
	Because I am seeing it in practice and have had numerous queries on all AML issues for the past number of years. There is still a lack of understanding as to what constitutes a "***reasonable risk based approach***" under AML. This leads to excessive and un-necessary collection and processing of personal data under data protection law, which is an infringement of the GDPR and potentially could be subject to DPC enforcement action and administrative fines.
10.	If you provide quote, mailshot customer every 12 months marketing and offering opt out - is this not sufficient to keep data?
	No. You have consent of customer to send them marketing information by electronic communications **only** but not to retain their personal data other than their email or phone number or other electronic means of communication.
11.	In funds, the contract is deemed to be entered when application firm is signed. if an investor 'quits' during AML/KYC process and never invests, should data still be held for 6/7 years in line with IFR and other regs?

If the investor never "invests" and has not supplied any money to the application firm then why is there AML collection and processing? Big difference in 'intending' to do investment with actually doing it. Is AML collection in this instance a 'reasonable risk based approach', if nothing of monetary value has changed hands?
12. Guidance from DPC re data retention of prospect clients would be welcomed - covering data in quotations, etc
This should be covered in our 2020 Annual report and the case study that I mentioned. Will be published in next few weeks.
13. What we're seeing in some cases when AML is being carried out as part of an onboarding process where a customer is using their mobile device is that there can be indiscriminate data ingestion of device data points to feed into risk determination. banks are not considering that such data should come under their risk assessments that need to consider necessity and proportionality.
A DPIA is essential to assess these risks and mitigate against these types of problems with proper safeguards to ensure there is no infringement of the GDPR for excessive or un-necessary collection of personal data. Failure to do a proper DPIA analysis, will likely incur greater action from the DPC in the event of an investigation of a complaint by our office.
14. Once again in relation to the Insurance Industry, they are using a Code of Practice on Data Protection that was last updated in June 2013. They dont seem interested or willing to update that and most companies in the sector are happy to do retention and other aspects guided by that CoP. What is the capacity fo the DPC to act on this?
WE are currently in advanced discussions with Insurance Ireland about a GDPR updated version of this Code of Practice which is a guidance document and we expect this to be published by II in the next month or so. In general, each of the Insurance companies are directly responsible for its own transparency and accountability in its data protection / privacy notices as required by the GDPR. If it came to our attention that any company was failing in its transparency requirements in some way then normally we would contact them, to address the matter.

15. Would CCR misreporting be considered a "personal data breach" considering that it would not arise from a "breach of security"?	
	See answer to 8 above
16. Where an Insurer provides a quotation but the policy was not subsequently incepted and the customer was given an opportunity not to receive direct marketing during the quotation process, the information provided may be used to direct market the customer the following year. The customer can be contacted again in subsequent years as long as they are given an opportunity to opt out at each contact and do not avail of this opportunity. Where a policy quote is not incepted, the quote can only be kept for 15 months to check against fraudulent applications. sorry, that's as per the Code of Practice on Data Protection for the Insurance Sector already in force.	
	This is under review (see Q14) as the Code is outdated and not compliant with GDPR.
17. The request for additional cdd and edd is proving difficult to implement whilst also balancing compliance with GDPR. Requesting something like Source of Wealth and Employment status is contentious but we have been advised it is a CJA requirement and CJA trumps GDPR... what is the DPC opinion on requesting this type of information.	
	As far as I understand, it is a requirement under AML to ascertain a person's source of wealth or income over 10,000 Euros when a payment is being made in cash. Or if the payment is from an unreliable source that requires Enhanced Due diligence because it is a suspicious transaction. If a proper explanation is not given by the individual then as far as I know, the service can/should, be refused and consideration should be given to reporting the matter to the FIU of the Gardai. Therefore, if it is a necessary requirement under AML then it will also be compliant with data protection laws. However, this should be done on a case-by-case basis and not through a "one size fits all" approach. If a large payment comes from another "Obliged entity" such as a bank a/c or trusted source then there is really no need to seek a persons source of income or wealth unless there are other factors that make the transaction suspicious i.e. PEPS.

18. The CBI stated in October that there is no de minimis amount in relation to screening against sanctions lists. How does this square with the message on GDPR?
Why is it necessary to profile an entire customer database against a sanction list if there are no suspicious transactions occurring? Again under data protection laws, it should be under a 'case by case', basis and the AML reasonable risk based approach where suspicious transaction have been identified based on country of origin of transaction or some other factors that require enhanced due diligence. In cases of a "de minimis" amounts there should be other suspicious indicators that require further assessment, before checking that particular **person**, against a sanction list.
19. Where are the main pitfalls/common themes by Firms that come through in complaints? What can we do to incorporate these into areas for improvement?
1. INACCURATE DATA – Not having the correct address or contact details for a person, which leads to unauthorised disclosure when sending mail, or ringing the wrong person. If a customer has not been engaged with for some time then you need to ensure that the records are updated and correct. 2. Failure to deal with Subject Access Requests (SARS) or giving improper or poor explanations as to why data is redacted or refused. 3. Unauthorised disclosures to third parties of any kind or without a proper legal basis 4. Using personal data for other purposes without an adequate explanation or legal basis. 5. Marketing without consent or failure to apply opt out
20. Where potential M&A's exist, as part of due diligence process, with NDA's in place, would legitimate interest a sufficient basis to allow specific data sharing for purposes of file audit as part of due diligence
I am not clear as to what this question is about but in general any exercise of a legitimate interest by a DC as a legal basis to further process personal data for other purposes has to be transparent, lawful and fair. ART 5.1 (a). Secondly and more importantly, it has to be balanced against the rights of data subjects, so that their rights and freedoms are not overridden by this further processing. I strongly recommend that a DPIA is done to assess these risks. Suitable, specific measures or safeguards should be identified and put in place. There should be a regular review by DPO or other competent person of this 'legitimate interest', processing.

21. Will GDPR Certification Schemes apply to financial services and all other organisations? Is there a timeframe to put Certification in place?
Work is in progress as to certification, which is an EDPB project, as it has to be consistent across all Member States. Check our website or media accounts for updates
22. Where a Data Request comes directly from a member of An Garda Siochána, should this not be actioned until such time as a Court Warrant or Garda Sergeant (or higher) is presented in writing?
There needs to be a paper record of any disclosure requests from AGS as otherwise it will be an un-authorised disclosure. Court Orders are not in the data protection remit and are exempted because court rules /procedures apply instead. A Garda may look at footage of CCTV but cannot get a copy of the footage without an official written request.
23. Are employment details not needed for AML CDD/ECDD, to determine if account activity is in line with anticipate profile for a customer?
Normally yes, unless there is a suspicious doubt over source of income from employment and the reasonable risk based approach applies. Again, it is a case by case rather than one size fits all.
24. Can I ask what opinion is on recording whether a person is Male or Female on an IT system where there is no option to record any other gender (in relation to Non Binary and other preferences)
Person has a fundamental right to object under Art 21 of GDPR and a right to rectification under Article 16. It does not matter if it is an automated IT system the data has to be corrected if the person provides evidence of correct gender. Equal Status Acts also apply, as this could be discrimination under gender status.
25. Where a customer submits a debit card disputed transaction form, claiming Fraud, would this require a breach report?
Potentially yes, if the subsequent investigation shows that there were unauthorised transactions from the A/c. These incidents are urgent as time limits of 72 hours apply when first notified of unauthorised access, to making a report to DPC.

26. What annoys/irritates DPO?
Lack of engagement by other units / staff / management in the company
27. Denis. Very interested in you and Gareth saying that the DPO is not the person to make the breach notification to DPC. Breach notification form asks specific question if it is the DPO making the report. Is there a conflict here?
DPO is the contact person with DPC but any compliance officer can make the breach report but should also inform company DPO.
28. What if the customer will not provide evidence of change of address and its only verbal instruction
Make a record/memo of the verbal instruction on the customers account as required by Article 5.1 (d)
29. can you share the questions and answers with all attendees as I would like to get more information on the AML side of things as that would be where the balance in complying with AML legislation and complying with GDPR is difficult to get the balance right.
Yes, it is difficult to get the balance right and we are open to further discussion on any new issues that you may wish to raise. Obviously, I am looking at AML through the view of data protection requirements. But there are several other parties who have a voice on this such as CBI, Dept of Justice, Gardai, private sector stakeholders, EU Commission etc. Nevertheless, fundamental rights have to be respected in any AML compliance.
30. Hi Garrett, you mention profiling in relation to AML data. Is screening for AML purposes really considered profiling in accordance with the definition of GDPR considering there generally speaking is a manual review of any AML risk classification?
Screening is *processing* of personal data. See definition of processing… ***means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;***

Profiling is defined as… means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; Normally there is some form of automated process in AML compliance processing. As far as I know, little case law defines exactly what is… *any form of automated processing.* However, in my opinion this could be subject to a wide interpretation especially when a DC is reviewing the characteristics of a person and their financial behaviour as required by the reasonable risk based approach under AML.
31. Can the commissioner give some guidance on over or un-necessary reporting as to how they will treat that.`
This is a work in progress and may be covered in the 2020 annual report as to the common breach type failures
32. What about keeping insurance quotation for 12 months to follow up before renewal due? Is that no longer allowed? Presumably if you have consent to follow up this would be ok?
If a contract is in place with the consumer then it could be retained for as long as is necessary and after the renewal date has expired, would seem to be the time when the old quotation is outdated and no longer required as a new quotation process is in place.
33. should an individual breach be reported?
See our guidance … https://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide
34. What effects does retaining information have on historic investigations to companies?
I do not understand this brief Q so I cannot give a response. If you wish to elaborate, you can contact me directly.

35. What about keeping insurance quotation for 12 months to follow up before renewal due? Is that no longer allowed?
See answer to 32 above. In addition, there should be good reasons as to why the quotation is being kept and what purposes it will be further used for and the consumer should be aware of this.
36. Why do the speakers believe the AML practioners hold AML requirements override DP requirements? Have been told this on several occasions also on training courses.
37. Question for Garrett: Can a bank claim "legitimate interest" (Art. 6 GDPR) for sharing personal data with a third party market research company for market research purposes, without having the data subject's consent, but mentioning this third party on their Data Protection Notice?
If the data being provided by the Bank to the Market research company is in an anonymous or pseudo-anonymous format that could not reveal the identity of the individual then there should be no issue. However if the data, does have personal information that could reveal the identity of the individual then this will be further processing and the consumer should be made aware of this as they have a Right to Object under Art 21 of GDPR or a Right to erasure Art 17, against the Market Research company. To avoid the potential of a customer exercising either of these rights then really the prior informed consent of the consumer should be obtained before any data is processed.
38. How do we manage the conflict around AML and GDPR data retention requirements?
A good retention policy is essential that examines what is necessarily required under AML to be retained.
39. What is your view on the Central Register of Beneficial Ownership (RBO) requiring PPSN as a means to verify the identity of the individual, rather than anything else, and in obtaining PPSNs, are sharing this info with Dept of Social Protection. And, as a non-Irish resident doesn't have a PPSN, this requirement is not applied across the board.

The Social Welfare (misc) Act 2005 permits certain public entities to collect the PPSN and process it, under specified circumstances (section 263). For non-residents who do not have a PPSN, I believe the process is to seek the Tax Identification Number (TIN) of the non-resident person. This is certainly true for CRS or FATCA reporting.

40. My question is therefore, fundamentally can AGS rely on S.41(b), as the 'statutory section' that applies or does Garrett agree with Denis that requests made by AGS citing section DPA 41(b), even where they also state the request is 'necessary and proportionate for preventing, detecting, investigating or prosecuting criminal offences', is inadequate for a Data Controller to respond to?

A disclosure to AGS based on a request from AGS citing Section 41 b of the Data Protection Act 2018 is not mandatory. Section 41 is a permissive provision, which states that a disclosure "shall be lawful to the extent that such processing is necessary or proportionate." A *prejudice test* is required to be undertaken by a data controller or processor based on these principles of necessity and proportionality. Overall, there should be consideration given as to whether there is a substantial risk that the purposes listed in 41(a) and (b) would be damaged by the data controller's failure to provide the information requested. However, the DPC acknowledges that a high proportion of requests for AGS to view or download CCTV may arise on foot of a DC instigating the involvement of AGS in the first instance in order to investigate incidents of a potentially criminal nature. In such circumstances, any disclosure of personal data by a data controller should nevertheless be underpinned by a precise legal basis. All disclosures should be recorded by the data controller in order to comply with records of processing activity requirements under GDPR and to demonstrate accountability.
On the AGS side, identification of the precise legal basis under which the data controller may make the disclosure strengthens the legitimacy of the data obtained and the making of requests in writing using official Garda communication channels demonstrates adherence by AGS to a common set of procedures. In compliance with the Data Protection Act 2018, all copies of data (i.e.CCTV footage) sought by AGS should be underpinned by a precise legal basis or on foot of a Court Order. Therefore, such requests by AGS can be refused by the Data Controller, if the AGS do not provide a proper reason(s) or if they have not been authorised by a Senior Garda (i.e. Superintendent). There is one slight exception to the rule, where there is an immediate danger to life or harm being caused to an individual and the situation requires urgent access.

Garrett O'Neill
18/2/2021

DISCLAIMER:- This correspondence is a general response to queries raised during the World Data Protection Day Seminar. It cannot elaborate in full on all the questions raised and it does not purport to represent legal advice or a full assessment of a complex area in law. Therefore any

recipients should seek independent legal advice before acting or refraining to act upon any guidance set out herein.