Transcript: Data Protection Commission Fines Confirmed 29 Nov 2022

Graham Doyle: Hello folks and you're very welcome to the Irish Data Protection Commission's latest podcast. My name is Graham Doyle. I'm Deputy Commissioner for Corporate Affairs, Media and Communications. Today I'm joined by my colleague and fellow Deputy Commissioner Cian O'Brien. Cian is responsible for the large scale inquiries and investigations conducted here by the DPC. So Cian, thank you very much for joining us.

Cian O'Brien: Thanks for having me.

Graham Doyle: Today what we're going to delve into 6 investigations that were conducted by the DPC over the last number of years. On Tuesday, the 29th of November, the Circuit Court here in Ireland has confirmed fines in each of the six cases. Cian, you're gonna speak to us about the inquiries, the outcomes, fines, and reprimands. But just before we get into the actual inquiries themselves, one of the questions I get asked regularly, in particular by the media, is where the fines actually go once confirmed by the courts.

Cian O'Brien: Thanks Graham. Now that the fines have been confirmed in the Circuit Court the next step is for the DPC to issue a notice requiring payment to each of the various entities. Those entities are then required to pay the money to the DPC within 28 days. At that point the DPC will engage with the Department of Public expenditure and reform for the purpose of remitting that money to the exchequer.

Graham Doyle: The six entities that we're speaking about were, Slane Credit Union, Meta Platforms Ireland Limited, the Teaching Council of Ireland, Bank of Ireland, the charity MOVE Ireland and then finally Limerick City and County Council. In addition to looking at the six entities in question, we'll also take a broader look in terms of what the six decisions and inquiries collectively tell us about the state of data protection, awareness, and enforcement here in Ireland. OK, let's jump straight into it. The fines involved ranged from the smallest which is €1500 to one of €17 million. So let's take a look at each of them in in in order. Can you recap the details please for us In relation to the investigation into Slane Credit Union?

Cian O'Brien: So this inquiry concerned the personal data breach by Slane Credit Union as a result of a technical issue on their website. Essentially what was happening was that Slane Credit Union was uploading reports to a part of their website that was intended to be accessible by the directors of the credit union only. These reports contained the personal data of applicants seeking to join the credit union. There was a plugin that was installed on the website to ensure search engine optimization and to help the website appear higher in search engine results. However, due to an error caused by an update to that plugin this meant that the reports in the director's area of the website started appearing in search engine results and were accessible via search those engine results. In terms of this inquiry, the important point to note is that the fact that the personal data breaches alone did not result in an infringement of the GDPR. But because there's no strict liability under the GDPR for personal data breaches, rather what the decision considered was the level of risk caused by the processing that Slane Credit Union was undertaking and whether the measures implemented by Slane Credit Union were appropriate in respect of that risk. So what the investigation found was that Slane Credit Union did not have its own risk assessment in place, it did not have a system in place for regular security checks on the website, and they did not have procedures in place to manage changes to the website. So for that reason Slane Credit Union was found to have infringed on the security requirements of the GDPR and was fined €5000. It was also reprimanded in this case.

Graham Doyle: Cian, can you tell us how to the DPC actually calculates that fine in terms of the infringement?

Cian O'Brien: There are a number of factors that set out in article 83.2 of the GDPR, that a supervisory authority such as the DPC must have regard to when calculating fines. Indeed it's important to remember that the overall objective, when calculating fines, is to arrive at a figure that is effective, proportionate, and dissuasive. So these factors include the gravity of the infringement, whether the infringement was intentional, any previous infringements, and many other factors that the DPC must have regard to. The DPC also has to have regard to the turnover of the entity being fined to make sure that any figure is proportionate to that turnover. I suppose though to outsiders it might seem a relatively small fine of €5000 when you compare it to the bigger fines that perhaps get so many of the headlines, in particular with the big tech platforms.

Graham Doyle: Would it be fair to say that it's down mainly to the nature of the infringement and the entity itself, or are their other mitigating concerns?

Cian O'Brien: It's really down to the specific detail of considering each of those factors set out in article 83.2 . For example, while this breach was very serious, it did not include financial data and Slane Credit Union was actually the first to discover the issue. They then took extensive steps to mitigate the issue once it had been identified. So those are factors that also have to be considered when balancing a proportionate response.

Graham Doyle: The final question then just in relation to this investigation Cian is, you said earlier that Slane Credit Union attributed the infringement to an update installed on its website. Is that a fairly prevalent issue that we see with organisations or that organisations themselves have to worry about?

Cian O'Brien: It's quite prevalent that technical issues, such as this, one can lead to personal data breaches. But it's also important to remember that the infringement of the GDPR was caused by a lack of appropriate measures to mitigate against that risk and technical issues like that. While the personal data breach may have been caused by the plug-in, the actual infringement for which Slane Credit Union was fined was caused by a lack of appropriate measures to mitigate against the risk.

Graham Doyle: We'll move on to one that the audience may be more familiar with because it's certainly the one that grabbed the most headlines of the six that we're talking about here today. That was the Meta case from earlier this year. We imposed a fine of 17 Million on Meta Platforms on the 15th of March this year. That decision followed an inquiry by the DPC which was initiated after we received 12 different breach notifications over a six month period. Can you give us some details in relation to the actual inquiry itself and the decision?

Cian O'Brien: A bit like Slane Credit Union this inquiry concerned personal data breaches that were notified by Meta to the DPC. In this case the breach concerned both the Facebook and Instagram services and indeed those breaches in this case were caused by software bugs that were code based. However, unlike the Slane Credit Union decision this decision did not find that Meta failed to implement appropriate security. Rather the infringement related to Meta's failure to be able to demonstrate the security that it had in place. A really important change that the GDPR introduced into data protection law is the

accountability principle. This requires that entities not only comply with the GDPR, but also that they can demonstrate that compliance. Meta's infringement related to this. For example, while Meta had policies in place for secure coding practices at the relevant time, it did infringe the accountability principle by failing to maintain records documenting adherence to those practices in the context of the 12 breaches. That's the reason why a €17 million fine was imposed in this case.

Graham Doyle: I wonder can you just tell us a bit more about what kind of data breach notification that we actually received that led to was opening this inquiry?

Cian O'Brien: Sure. The software bugs in this case caused a range of different issues for confidentiality of data. In some cases the bugs allowed users who had been blocked by other users to see that users posts or indeed to message that user. In other cases private Instagram accounts became public and there were some other issues around information being shared with a wider audience than intended by the Facebook or Instagram user.

Graham Doyle: Let's move on then to the third one which is to do with the Teaching Council of Ireland. As people no doubt are aware the Council promotes and regulates professional standards in teaching. This is an inquiry that was initiated by the DPC after the Teaching Council notified us of a personal data breach on the 9th of March in 2020 and it was finalized on the 2nd of December of last year 2021. Could you give us some insight into this issue?

Cian O'Brien: This is a good example of an inquiry whereby the personal data breach was caused by a malicious external actor. Essentially, that malicious actor sent assisting e-mail to the Teaching Council and the Teaching Council inadvertently engaged with that e-mail. The result of engaging with that e-mail, automatic forwarding rules were applied for emails from certain accounts to the malicious actor. In total 323 emails were forwarded to that malicious actor and unfortunately one of those emails included a spreadsheet containing the vetting status of almost 10,000 teachers. Again the decision considered the level of risk caused by the teaching councils processing and whether the measures implemented by the Teaching Council were appropriate to address that risk. Crucial to this decision was the fact that there were a range of measures that the Teaching Council could have implemented to mitigate the risk of these types of breaches occurring. They could have for example implemented restrictions on auto forwarding rules on e-mail accounts. There were also more secure methods

for transferring personal data, for example the Teaching Council was sending personal data and spreadsheets by e-mail in an unencrypted format and without password protection. So there were a range of measures that the Teaching Council could have implemented to further mitigate the risk of unfortunate phishing incidents like this one. In those circumstances the Teaching Council was found to have infringed the security principles. They're also in circumstances found to have infringed Article 33 which requires that personal data breaches must be notified to the data protection Commission with add undue delay so there are two separate fines imposed in this case, totaling €60,000. Importantly there was also an order imposed in this case which ordered the Teaching Council to take specific steps to bring its processing into compliance, in terms of the issue of auto forwarding.

Graham Doyle: How common is it and from your experience here in the DPC, for auto forwarding to lead to a data breach?

Cian O'Brien: in terms of the cases that we've seen certainly it is very common. Phishing attacks are also very common indeed. This is where an attacker uses fraudulent emails or messages to gain access to data. This can take the form of auto forwarding rules, as was the case in this particular inquiry. But attackers also use a variety of different techniques to gain access to that data, so it's really important that staff are vigilant and receive appropriate training on how to recognize phishing attacks. The DPC currently has another inquiry open which is somewhat similar and concerns auto forwarding rules. So unfortunately it is very prevalent and indeed some of the phishing emails that the DPC are seeing are very sophisticated.

Graham Doyle: We might move on now to the 4th inquiry and that's the one involving the Bank of Ireland. This was an inquiry that was commenced after the Bank of Ireland Group made 22 personal data breach notifications to the DPC between the 9th and November 2018 and the 27th of June 2019 and these notifications related to the the information Bank of Ireland feed to the Central Credit Register. Could you talk a little about the investigation and the fine that is being imposed and confirmed by the court?

Cian O'Brien: What this inquiry mostly concerned was inaccurate information being submitted to the Central Credit Register. Of course financial service

providers are obliged to submit certain information to the Central Credit Register and the CCR uses this information to compile credit reports on individuals. Most of these breaches related to inaccurate information being shared rather than the fact of the sharing alone. One point that Bank of Ireland emphasized during the inquiry is that it's not possible for any credit provider to operate on a zero error model in this regard, and the decision as a result considered the level of risk caused by the processing and whether the measures implemented by Bank of Ireland to address the risk were appropriate. In terms of the findings made in the decision, the decision found that Bank of Ireland infringed the security provisions of the GDPR by failing to implement appropriate measures. For example there is a lack of validation procedures to verify the accuracy of data prior to being transferred to the Central Credit Register. There's also a lack of appropriate training for staff to ensure that the information that was transferred was accurate and necessary. In this case as well as that infringement of article 30 requirements, Bank of Ireland also infringed articles 33 and 34 of the GDPR. Both by failing to notify the DPC of certain breaches on time and also by failing to notify data subjects of certain preachers without delay. The decision imposed a number of fines totaling €463,000 and it also ordered Bank of Ireland to bring its processing into compliance by taking certain steps to increase the security of the processing.

Graham Doyle: At the outset of this I said that there were 22 personal data breach notifications made to us but if I'm correct three of those 22 didn't meet the actual criteria for personal data breaches. So what kind of breaches were they?

Cian O'Brien: That's correct three of them didn't in this case. I think this decision is actually quite helpful for defining what constitutes a personal data breach under GDPR. It is a very broad definition and as I mentioned earlier a personal data breach isn't an infringement of the GDPR, but it does create certain requirements, certain obligations on controllers in terms of how they respond to personal data breaches. What's important to take from this decision is that personal data breaches include instances where information is changed to make it inaccurate, so when we're talking about personal data breaches we're not just talking about unauthorized disclosures of data, but also where data has changed to make it inaccurate. This can also constitute a personal data breach. In this case Bank of Ireland notified the DPC of 22 personal data breaches and it's important that they did so because there is a 72 hour period in which

controllers have to notify personal data breaches to the DPC from when they become aware of it. However, in three of those cases Bank of Ireland was subsequently able to confirm that the information shared with the CCR was in fact accurate. So at the time of notification, within that 72 hour period, it appeared that a personal data breach had occurred. Bank of Ireland took the correct approach by notifying those breaches to the DPC. It was subsequently able to provide an update to the DPC upon further investigation which clarified that the information submitted in those three cases was actually accurate so that no personal data breach occurred. As you said earlier the notification requirement for the DPC 72 hours. Where the harm could arise for an individual however was that they did fail to notify data subjects in a timely manner. That's where the risk can cause serious harm. I this type of processing concerning registers where an individual may have been denied credit based on inaccurate information, notifying data subjects obviously can have a significant impact on mitigating the risk to those data subjects. You can then take appropriate action to correct the inaccurate information.

Graham Doyle: The CCR is used by other financial institutions, isn't it, and had there been other data breaches relating to its use that we've seen there have indeed so it's used by all financial service providers regarding loans worth €500 or more and we have seen a variety of breaches concerning a variety of different financial institutions. Not only financial institutions, but we've also seen another credit rating agency the Irish Credit Bureau having similar personal data breaches in terms of their own internal systems and the accuracy of data. The Irish credit Bureau was fined €90,000 by the DPC last year for those infringements of the GDPR and that was confirmed by the courts in 202. That money has since been collected and remitted to the exchequer. Obviously Cian, it's down to individual financial institutions to protect customer's data when they use outside organizations, but I suppose can you offer listeners some reassurances in terms of what we hear at the DPC have noticed what lenders are doing in this regard?

Cian O'Brien: Absolutely, I suppose specifically in this case, the DPC did order Bank of Ireland to implement specific measures to protect data and the DPC's enforcement unit has followed up with Bank of Ireland to ensure compliance. I suppose more generally the risk based approach that's provided for under the GDPR requires that the appropriate security must be continually reassessed by all entities including financial institutions, such as this one, to ensure that the

standards implemented is appropriate to the risk. There's an obligation on entities to continually seek measures to improve the security and accuracy off their data. One other point I would make in this regard, in terms of any data subjects that may have concerns, is one of the important changes brought to data protection law by the GDPR in 2018. It ensures that entities cannot charge a fee for subject access requests of this nature. Individuals are entitled to a copy of their credit report for free so if anybody has any concerns about the accuracy in respect of that data they can check for free by requesting a copy of their credit report.

Graham Doyle: So can you talk about the second last inquiry. The decision confirmed by the court is an inquiry into the charity MOVE Ireland. Some listeners will be familiar and others may not in relation to MOVE Ireland. It's a registered charity and the charity itself supports the safety and well-being of women and their children who were experiencing, or have experienced, violence or abuse in an intimate relationship. MOVE Ireland notified the DPC of a personal data breach in February 2020. I wonder if you could again, like the other ones, just talk us through the breach notification we received, the inquiry, and ultimately the fine that's been confirmed?

Cian O'Brien: Sure, so as part of its work MOVE Ireland made video recordings of group sessions in which facilitators engaged with participants and encouraged those participants to take responsibility for their violence and to change their behavior. Unfortunately, the charity lost 18 SD cards containing these recordings and of course those recordings may have included sensitive data relating to the participants the facilitators and indeed victims of domestic violence. This decision considered the level of risk caused by that processing of personal data and whether measures implemented by MOVE to address the risks were appropriate. The decision found indeed that MOVE Ireland failed to implement appropriate security in respect of this processing and in particular there was a lack of oversight of the procedures that set out how personal data was processed, retained and deleted on those SD cards. There was a lack of organisational measures that enabled MOVE Ireland to test assess and evaluate the effectiveness of those measures and there was also a lack of training for facilitators on those data protection requirements. In this case the data protection Commission imposed a fine of €1500 and crucially it also imposed an order on MOVE Ireland to take specific steps to secure the ongoing processing of personal data.

Graham Doyle: That's great thanks for covering that one off. We'll move on to the final one which was the decision and fine by the court in relation to Limerick City and County Council. Again this was an inquiry that the DPC has set up as part of a range of inquiries that we have into local authorities in terms of surveillance. Could you give us a bit of background on the inquiry?

Cian O'Brien: This was one of a number of audits into the 31 local authorities examining the lawfulness of state surveillance for law enforcement purposes. These inquiries really concerned technologies such as CCTV, body worn cameras, automatic number plate recognition, drones and other technologies. The decision made a large number of very comprehensive findings in this case, such as the decision found that certain CCTV cameras were unlawful because they had not been authorized by the Garda Commissioner as required by An Garda Síochána Act 2005. It also found that the council's use of automatic number plate recognition was unlawful because it lacks an appropriate basis in law. In total the DPC imposed 3 fines totaling €110,000 and it also imposed a temporary ban on certain processing for CCTV cameras at a number of locations until such time as a an appropriate legal basis can be rectified. It also provided Limerick City and County Council with a detailed order requiring it to take certain steps to bring its processing into compliance and it also imposed a reprimand on Limerick city and County Council.

Graham Doyle: This really was a very comprehensive decision in terms of CCTV cameras because I know this is an area that gets an awful lot of attention. Dealing with the domestic media, it's an area that I regularly get contacted in relation to. In terms of the cameras themselves can you distinguish first between what public authorities such as Limerick city and County Council are allowed to do visa what members of the public are permitted to do?

Cian O'Brien: If the purpose of CCTTV is for law enforcement purposes that means that the same rules apply to An Garda Síochána, public authorities and local authorities. Those rules are set out in the Law Enforcement Directive rather than the GDPR .The Law Enforcement Directive deals with processing of personal data for law enforcement purposes. This applies to local authorities where they are processing for purposes such as preventing or detecting crime. A key point here in terms of having a lawful basis under the Law Enforcement Directive is that there must be binding rules setting out when such surveillance technologies can be used either by An Garda Síochána or by the local

authorities. These rules must be clear, they must be precise, and they must be foreseeable. By setting out these rules it brings clarity to when the surveillance technologies can be properly deployed and in turn limits the discretion for arbitrary interference or for arbitrary surveillance.

So I think a very good example of this in practice can be seen in an earlier DPC decision concerning Kerry County Council in 2020. This decision concerns the use of CCTV to prevent and detect littering which of course is a law enforcement purpose. The decision found that there was no basis in law for this surveillance because there were no rules setting out with clarity precision and foreseeability when the technology could be deployed and when the technology cannot be deployed. However, since then the Oireachtas has enacted the circular economy act which seeks to provide those rules to provide clarity as to when CCTV can be used for littering purposes. That type of oversight really is crucial under the law enforcement directive.

Graham Doyle: Cian, what about me as a homeowner? When we talk about CCTV can you outline what is and what's not allowable when it comes to me and protecting my own private property?

Cian O'Brien: The rules are very different when it comes to homeowners because the GDPR is applicable. Because we're not talking about law enforcement, crucially GDPR has a household exemption which can apply to domestic CCTV. This means that if a domestic CCTV system is operated in a way that it only captures images within the perimeter of the CCTV owners own property then that household exemption can be applicable and such the GDPR does not apply in that case. Such processing and such use of CCTV is entirely lawful.

Graham Doyle: The final question in relation to Limerick City and County Council, the inquiry and the decision. As you said earlier the DPC imposed the fine of €110,000. That's actually only over 10% of what we could have imposed in this in this decision. Can you explain just the difference between fines and when you're talking about fining a public authority to be a private sector organization?

Cian O'Brien: You're absolutely correct. When fining a public authority the Data Protection Act of 2018 limits to DPC to a fine of a maximum of €1,000,000. The fine imposed on Limerick city and County Council represents over 10% of the

maximum. However, when fining other entities the GDPR sets out the relevant caps. Indeed the caps are significantly larger in that they're higher depending on the type of infringement. Either 2% of the entities turnover or €10 million or indeed for other infringements it's the higher of 4% of the entities turnover or €20 million. I think that's important because there has been a lot of conversation in the past, certainly around the time when the GDPR was introduced. The DPC's positioned at the time was it was very important to have some sort of fining mechanism because it actually adds a level of accountability.

Graham Doyle: Thanks very much for that. As we said at the outset these six fines that have been confirmed in the Circuit Court on Tuesday the 29th of November, is there anything that stands out to you about these fines or reprimands? For instance do you notice any source of patterns or does each individual find tell its own story? I think our listeners would be very intrigued to hear kind of any tips that we might have.

Cian O'Brien: From what we see I think one of the first points that stands out for me when looking back on these mixed decisions is that the fines really represent the extent of regulatory role that the Data Protection Commission has. The entities involved include diverse entities such as technology companies, to charities, to financial institutions, to public bodies and all of these entities are required to implement measures to ensure compliance with the GDPR. I think these decisions give us a good example of inquiries where DPC has taken on its own initiative to look into the lawfulness of certain processing and also inquiries showing the DPC's response to personal data breaches. I think, as well, the six decisions when considered together provide a good example of how the GDPR adopts a risk based approach. These decisions really give insight into what that looks like in specific circumstances and I think it's particularly helpful to read these decisions alongside two other decisions that the DPC recently published on its website concerning Ark Life and Allianz. These decisions also concern circumstances where personal data breaches were notified to the DPC. However, in each of those two decisions the DPC found that the measures implemented by Ark Life and by Allianz were appropriate in light of the risk of the processing, so no infringements were found. Today we've been talking about the fines and of course they occur where infringements have been found to have been occurring. In these two cases no infringements were found because the level of measures implemented were appropriate to the risk. So, I think it's helpful to compare the different decisions for entities trying to understand what

is an appropriate level of security, in light of their individual processing operations and in terms of best practices. I'd say that the first step in implementing appropriate security is to undertake a risk assessment to understand what the risks are and then to implement appropriate measures based on that risk assessment. Finally, I want to mention the accountability principle. This will certainly also in play in the decisions we've discussed today. That's a crucial new change under the GDPR, as entities must ensure that they can demonstrate compliance not only that they comply, but also document what measures an entity has in place, and indeed to document how those measures are implemented in specific circumstances, especially when something goes wrong.

Graham Doyle: Just when you talk about the Ark Life and the Allianz case. I've been at a couple of events recently where stakeholders were commenting on how useful it is to see and to see the decisions out there. We've been talking through six decisions here with fines in relation to breaches and infringements of the GDPR. However, quite often stakeholders are asking us what does 'good' look like. So I do think that the examples that you mentioned of Ark Life and Allianz are important. There's learnings from where an organization has had an issue, but has dealt with it, from our perspective as the regulator in a really good way. So Cian, thanks so much for bringing your expertise and your knowledge to this today.

I hope you the listeners have found it useful and until our next podcast, thank you,