Transcript: Data Protection Day 2023 - FAQ Podcast

Graham Doyle: Hello folks and welcome to the Data Protection Commission Podcast. My name is Graham Doyle, I'm Deputy Commissioner and Head of Communications here at the DPC.

Today is January 28th and it's also Data Protection Day, marking 42 years since the signing of the first pan European Data Protection Framework Convention 108. It's also the fifth year of the implementation of the GDPR or the General Data Protection Regulation. A lot of the language surrounding data protection and the GDPR can be complicated and off putting at times often leaving individuals and organizations confused about their rights and obligations, in everyday situations such as contacting service providers using social media platforms applying for a job or even just going shopping. Here at the DPC we take note of the trends on topics that we see most coming through our helplines, e-mail, in our external engagements and even in the online discussions that take place when we're monitoring our Twitter and LinkedIn accounts. We are going to take a look at some of these frequently asked questions today. I'm delighted to be joined by my fellow deputy commissioner Ian Chambers. Ian is the head of regulatory activity here at the DPC and it's great to have you today, especially with your extensive experience leading what was is the DPC's information and assessment units. I'd like just to start off with a very basic and obvious question what is personal data?

Ian Chambers: It's great to join you here today to have a chat about a few of these that we see coming up. Personal data basically means any information about a living person where that person is identified or could be identified or identifiable. Personal data can cover various types of information such as name, date of birth, e-mail address, phone number, address physical characteristics, location data. It's quite wide-ranging. Once it is clear to whom that information relates or is reasonably possible to find it out it doesn't have to be written in form it can also be information about what a data subject looks or sounds like, such as photos or audio or video recordings. But data protection only applies when that information is processed by automated means such as electronically or as part of some other kind of filing system. It's limited to a living person. The personal data of someone who's deceased or passed away is not covered by the GDPR and as a result we can't give assistance in those kind of cases. However if

somebody does have a query or complain about their own personal data they can contact us through our web forms or by calling our help desk.

Graham Doyle: Great and I'll give that all the details at the end of the podcast. Could you speak about some of the terms that are commonly used in the data protection world which pop up a lot on our website? Can we start off by explaining what we mean when we say the data subject and what does that mean?

Ian Chambers: A data subject is simply an individual or the owner of personal data, the information that's being processed by a data controller. It is an individual generally speaking, although in some instances the data controller can also be in an individual. But in plain terms it's any of the people out there whose personal data is being processed or held by an organization.

Graham Doyle: You've mentioned data controller, so what is a data controller?

Ian Chambers: A data controller is a person, a company or body that decides how and why that data subject's personal is processed. Sometimes you have two or more persons or entities that make these decisions and they would be joint controllers in that case. Both controllers would share responsibility for the data processing obligations. Generally speaking a data controller is an organization but, as I said previously, it can be an individual.

Graham Doyle: I think at times there is a bit of confusion out there because we've got data controllers and then we've also got the data processor. We get quite a lot of queries into the DPC where people are querying what the difference is. So can you tell us how a processer are different to a controller?

Ian Chambers: Some of the terminology can be confusing. We've got processors and we've got processing of personal data. The processor refers to a person or a company or any other body which processes personal data on behalf of a controller. The important difference there is that they don't decide how or why the processing takes place but instead carry out the processing on the orders of the controller. That's often where a company engages the services of another company to carry out some activities for them on their behalf. Your rights in relation to data, your data, being handled by a data processor are quite different in terms of your relationship with them. For example if you wanted to see what personal data relationships being held by a data processor you would make an access request to the data controller engaging their services and not directly to

the data processor. That's an important point as we see people often not being clear, or it not being clear to them, who they should make that request. It should be clear under the transparency obligations for data controllers when they're engaging the services of processor, but it's something we see coming up quite commonly, people making access requests to a processor. It's not the processor who should be filling that, it's the data controller who's employing that processor.

Graham Doyle: In those circumstances where somebody comes to us and says they try to make an access request through processor and maybe are not getting anywhere. What advice do we give them at that point in time? Go directly to the controller?

Ian Chambers: Yes, that's your first port of call in relation to it and then the controller should then engage with the processor to get any personal data that's being requested. It should be coming through the controller, as the controller is the person or the body or the organization that's meant to facilitate the access request. For example, if I'm an individual dealing with an organization, anything that's happening in the background in terms of the processor relationship with your organization, that organization deals with that. This is designed to make things easier for you as a data subject. It's who you have the relationship with. So if you engage with the banking service, they may have multiple processors processing my personal data such as IT systems or banking systems or financial systems. It shouldn't be on me as a data subject to have to figure out who all these individual organisations are, go to them individually and make the data access request. I make my access request to the organization that I have the business relationship with, the contractual relationship or whatever other kind of relationship. They then in turn get all that information collated and give it to me, as is my right under the GDPR.

Graham Doyle: That's an important example that helps explain the distinction between the processor and the controller. Can you remind our listeners of the obligations in terms of time frames etc when handling subject access requests?

Ian Chambers: Controllers have one month to respond to an access request received. There are certain circumstances or instances for example where it's a high volume, or a technically complex exercise in terms of fulfilling an access request, where they can take another two months. But a key part, if they are going to take an additional time, they have to tell the data subject within that

first month. They have to explain to them why they're doing so. But generally speaking the standard is one month to get a reply. What may create the requirement for that two months is if there's, a back and forth or clarification that's needed about what kind of personal data is being sought. There can also be clarifications sought about what is or isn't their personal data which can sometimes not be as clear as people might think. It may be a partners or spouse's information mixed in there, or business partner, or something of that nature. They will clarify what is and isn't releasable under an access request. That process can sometimes take some time and we would encourage engagement between the data subject and the data controller to facilitate an efficient handling of the personal data.

Graham Doyle: We might move on just to the right of an individual or a data subject. What rights are included under the GDPR?

Ian Chambers: A data subjects rights include, the right to be informed if, how and why your data is being processed, the right to access or to get a copy of your data, the right to have your data corrected or supplemented if it's inaccurate or incomplete, the right to have your data erased, the right to limit or restrict how your data is used, the right to data portability, the right to object to the processing of your data and the right not to be subject to automated decisions. The most common would be the right to access, right to rectification and the right to erasure. Those are the ones we see coming into us when people are looking for access to their personal data people. Rectification is an important one to mention because your right to rectification is when there's a factual error. This is if your name is spelled wrong or your date of birth is incorrectly recorded. This is not a right to rectification in relation to the opinions of a third party and some kind of report.

None of the rights that are provided for the GDPR are absolute and that's an important thing to be cognizant about. We are always very happy to explain to what extent the right applies via or help desk or e-mail or our web forms. We find ourselves often having to explain to what extent those rights. For example, if you've got a relationship with a bank, they have a personal data related relationship, they also have legal obligations in relation to the retention of that personal data. That means if you look for them to raise all your personal data they're not going to be able to do so because they have to comply with their legal obligations. Equally if you were looking to get your tax records erased from

the Revenue Commissioners, they're not going to comply with that even though you have a right to erase under GDPR. At the same time they have contravening legal obligations on their part in relation retention of your personal data.

Graham Doyle: We're gonna be launching our Annual Report for 2022 in late February and year on year access requests are a significant majority the type of complaints that we receive. No doubt that trend has continued in 2022. Can we now move on now to explain to individuals out there if they have a concern that their rights aren't being followed and what steps can they take? Obviously you deal with making a complaint through the DPC but even in advance of making a complaint to ourselves, what practical tips can you give?

Ian Chambers: In relation to the exercising of rights to an access request, rectification requests or erasure requests. This may seem to be the first step for some people, but it's not. The first step in every instance to contact the data controller directly in writing. You have a right to make any of these requests verbally but what could be problematic down the line is if there's no record of this verbal request, which impedes our progress on the complaint. If there's no record of you having made the request, this can take away our investigative processes or our complaint handling processes.

If a person or data subject wanted access to any of their information or their personal data being held by a controller and they make an access request, it's important to remember that the data subject is only entitled to their personal data in relation to access question and not to entire files or to other people's personal data or non-personal data or indeed original documents. So if you were to make an access request to a bank who have your mortgage deeds, they can give you a copy of your personal data. If you are seeking the original, that's an entirely different process that you may need to go to the courts or have a solicitor make the request on your behalf.

We would also always ask that when somebody's making a complaint and have been responded to, a copy of that access request will be essential. We need this for a variety of reasons and we can't move a complaint forward without it. So , in every instance when somebody is getting on to us and they have a concern and try to exercise their rights the first thing we'd asked to send it into us, along with the web form or the e-mail, is a copy of the request that they've made. This is very important for us to be able to move things on as efficiently as we can.

Graham Doyle: I think it's a very good piece of advice to give to individuals. Quite often we read on social media where people are talking about the fact that you don't have to make access requests in writing, but it is good advice. As it is very helpful for us and when an individual has gone and done that and could provide a bit of evidence. It's an important starting point for us in terms of when we go and examine the query or complaint.

Ian Chambers: 100%, you have a right to exercise your rights under the GDPR verbally. But where this can turn into an issue is further down the road. We see this often with smaller businesses or organizations. Such as, you go into the shop and say I want access to some CCTV footage and they don't give it to you. Then you come back to us somewhere down the road and inform us that you made an access request to this organization. Then it turns out that they have no records or maybe the person isn't working there anymore and they have no way of verifying or confirming that the access request was actually made. That leaves us little stranded in terms of how we can progress and get you access to your personal data. So absolutely 100% you can make it verbally. But best practice, and for better efficiency and the better handling of complaints on our end, is to ensure we have a copy of the request that you've made. This really helps move things along.

Graham Doyle: I've seen some commentary on social media in particular where individuals think that under the GDPR consent is needed very time your personal data is being processed. But this is not the case. Could you give other examples where people might benefit from some clarity in this area, from what we we've seen over the over the years here in DPC?

Ian Chambers: Yeah absolutely. I suppose it's one of the most common misconceptions out there that your consent is required for the processing of your personal data. There are actually six lawful basis set out of the GDPR that allow the lawful processing of personal data. The GDPR doesn't prevent the processing of personal data, it just requires that it's done lawfully. Most of what we do in life is gonna be processing of personal data such as adding points to a Tesco Club Cards, to paying your mortgage, or signing for delivery. in the The issue we see again and again is that not everything going wrong in terms of interaction you have with an organization or business is a data protection issue, even though it involves the processing of personal data. Sometimes it's part of a much wider issue that can't be resolved by the DPC. The processing of personal

data happens in nearly every walk of life and nearly every interaction that you have with an organization or a company or business there's going to be some processing. Such as your name, telephone number, e-mail address, financial information or some other information. Often data protection is not the central pillar of that problem. You may be getting poor customer service. The customer service element of that relationship between the individual and the organization quite often is the issue that's at play. The vehicle for which the individual will try and resolve the issue is by going to the company, lodging a subject access request, where they want to get the correspondence or access to the phone call that they've had that that's been problematic.

Graham Doyle: This is an important take away for controllers. If you're not giving people information that they're entitled to and if you're forcing them down a formalised route like an access request to get information that you should be freely giving to them in the first instance. If people feel they have no ability to go that information other that a formalised route then I think that's not satisfactory for the data subject or the data controller. If people are given information at the front end and if they're responded to properly then it avoids the DPC becoming involved which is better off all around for people.

The transparency piece of the GDPR is also essential. When interacting with data controllers the number one thing I always say to them it's the more transparent and the more information you give to people, the better off for everyone. They will get less complaint and less issues arising. Transparency is the is the key piece for me when we say not everything that goes wrong is data protection issue. We see this a lot when it comes to CCTV. Could you briefly talk to us about what we see when it comes to CCTV issues?

Ian Chambers: CCTV is probably one of the more contentious ones. But when I'm talking about CCTV here I'm not talking about commercial CCTV, which is a different matter. What I'm speaking about here is CCTV in a household that people might have in their homes and for their own security. CCTV is a good example of where there's a complaint about CCTV and it tends to arise due to a dispute between neighbors or threatening behavior or criminality. Once that underlining dispute resolves, often the data protection issue resolves. Equally the DPC can't resolve the underlying issue of criminality. If there's a dispute or an extreme disagreement over land, if there's a dispute as to who owns the right of way on a property, that's not the role of the DPC to decide.

Another one that we see a bit of is disputes between parents over images of their children. If they're no longer together those pictures being put up on a private social media account and one party is objecting picture that the other party put up. Again, that's private social media the DPC doesn't have a role in addressing that kind issue. The domestic exemption would also feature in relation to CCTV if the CCTV is capturing within the confines of somebody's property. We are not the CCTV regulator we're the Data Protection Commission. The GDPR doesn't apply to the processing of personal data within the confines of somebody's home and so that those are the household exemptions. Everyone processes other people's personal data within their day-to-day that doesn't make them a data controller, as defined by the GDPR. I'm talking about the uploading of photos as an example. If someone uploads a photo to their private social media accounts the GDPR doesn't apply. Generally speaking a private social media account with limited just friends and family tends not to fall under the under the GDPR. In terms of that individual, the platform is absolutely subject to the GDPR. A social media platform is subject to GDPR and any process that the individual that's using the platform as a person may not be deemed to be a data controller. Look, the GDPR is still fairly new and there's some what I'm talking about today is off the back of the actual court rulings. If you are broadcasting it all for the world to see, then you're getting into a different area, and you may actually become a controller. More importantly the platform may actually may be subject to the exercising of some its GDPR rights there.

Graham Doyle: In those cases where data protection isn't the central issue, what should an individual do? What advice would we have for an individual?

Ian Chambers: If the underlying issue may be more appropriately addressed by another regulatory body like the Medical Council or the Competition and Consumer Protection Commission, or others, depending on the details and the circumstances. There are also times when someone makes a complaint that would be more appropriate for our DPC Supervision Unit. For example, biometric data in the workplace where the person who's raised the concern with us, but hasn't actually provided a handprint or facial scan, so there hasn't been processing with their own personal data that we could we could pursue a complaint. This is special category data, which biometric data is. It would be

more effective to address this not by way of the complaint, but by directly engaging with the data controller. Where there's an issue involving a vulnerable person who may not be able to make a complaint themselves, in say a hospital, we would engage directly with the hospital via our supervision and consultation team to ensure that they're processing data correctly and in line with GDPR.

There are times where a concern that's raised with us is a valid GDPR concern, but it's not appropriate for us to get involved. A case may be currently active before the courts or the Tenancy Board or the WRC. In those situations the DPC might be in the position to examine the concern that's raised with us.

Graham Doyle: In the final question, me as an individual if I don't know what personal data is being processed or if I don't know what personal data is being processed by a particular organization, but I think that they are processing personal data about me. What should I do?

Ian Chambers: Data controllers have obligations. Article 12 of the GDPR that sets out how a data subject can exercise their rights. One of those rights states that data subject should have the right to obtain from the controller confirmation as to whether their personal data are being processed. Even if they're not processing personal data they must respond to the data subject, stating the same. That means whether the organization is processing your personal data or not, if you make an access request they have to respond to you.

Under the GDPR there's six possible legal basis for processing personal data. In terms of legal basis, also referred to as a lawful basis or lawful reason, means the legal justification for the processing of personal data. For a person's data to be lawfully processed in line with data protection, the controller must have a valid legal basis and this information should be provided to data subjects upon request, as part of the principle of transparency. We Transparency it is a key, as controller's should always be able to identify the legal basis they're relying on for processing if asked by data subject or the DPC. Information provided must be transparent, understandable, easily accessible, clear and in plain language. The information should be provided in writing or in an appropriate means. That is depending on the matter in which the person makes the request or if they can request it to be transmitted to them via the alternative means. Data controllers also have an obligation to make sure your personal data is kept secure, so they have obligations to ensure that if somebody contacted them making an access

request that they verify that that person making the access is the is the data subject. People can find this little frustrating at times and there can be issues where data controllers are asking for too much information.

It’s legitimate for them to confirm your identity, because if they don't and then send the access request information and it's not you that's making the ask, they’ve just committed a data breach. It’s also important to note that they shouldn't be asking you for information to confirm your identity, that they don't already have. So they shouldn't be asking you for a copy of your passport if they don't already have a copy of your passport. Now alternatively there can be circumstances where at the start of the relationship they ask you for a copy of your passport and that may be legitimate. This depends on the relationship depends with the organization and how you're interacting with that organization. But in terms of you making an access request, generally speaking, if they're asking for information to confirm your identity it should be information that they already hold.

Graham Doyle: I think that's a great place to finish off today. There was a lot of information to take in, so I hope the listeners find it useful. All of this information that we've gone through today, and along with our web forms that you mentioned earlier, are available on our website. Just reminder to listeners, our website is www.dataprotection.ie. Our helplines are open Monday to Friday from 9:30 AM to 1:00 PM and again from 2:00 PM until 5:30 PM. The number that you can contact us on are 01 7650100.

Many thanks again for joining me here today it's been very useful and happy data protection day to all our listeners!

Thanks very much take care.