[00:00:00.250] - Introduction

In the third panel discussion at the Digital Reform: Insights and Regulators' Perspective Seminar, Aoife Mac Ardle moderates a discussion on "Online Content: New Areas of Regulation." The legal context for the discussion is the GDPR and the Digital Services Act, and the topics include children's data, harmful content as it relates to children, online advertising and sponsored content, dark patterns and operational compliance under the Digital Services Act.

[00:00:30.030] – Aoife Mac Ardle, Senior Associate

We're going to take a look at some of the new areas of regulation we discussed earlier in a little bit more detail. I'm joined on stage by Aoife, Alison, David and Lorraine and all of us are Associates in the Technology Group. What we're going to look at today are some topics that have traditionally been hot areas under data protection and then see how these concepts, like children and online advertising are addressed under new forms of regulation. We're also going to dip into the operational side of compliance to see what the picture looks like and how you might be able to leverage some of your existing data protection compliance to meet these new obligations. There's going to be some detail in the discussion, so you're welcome to take notes as we go, but equally feel free to just sit back and listen to the discussion. So, to kick things off, we're going to look at our first regulatory theme and it's one that was covered quite a bit in the session earlier about protecting children online. I'm going to come to you first on this Aoife. I know in the panel earlier we heard about regulatory cooperation and how this fits with protection of children and we know that children's data has traditionally been an area of interest for the DPC.

[00:01:38.390] – Aoife Mac Ardle, Senior Associate

So I was wondering if you could take us through in maybe a little bit more detail what measures have been played out in that area?

[00:01:45.330] – Aoife Coll, Associate

Sure, thanks Aoife. I'm just going to speak a little bit about the "Fundamentals". So the DPC's fundamentals for a child-oriented approach to data processing, or the "Fundamentals" for short, were released in December 2021. They were released after a detailed public consultation, including with children so the DPC engaged with kids through their teachers, their parents and guardians, and also through youth groups. The Fundamentals apply to online and offline services that are intended for, directed at or likely to be accessed by children. The regulatory focus on children is not limited to the DPC and the Information Commissioner's Office in the UK

has also released the Children's Code and both the Fundamentals and the Children's Code categorise persons under the age of 18 as children. So the Fundamentals set out 14 fundamentals that organisations that process children's data are supposed to comply with, and the principle of the best interest of the child underpins all of the fundamentals.

[00:02:41.590] – Aoife Mac Ardle, Senior Associate

So of the 14 fundamentals that are covered by the DPC, what are the really key points that are coming out of those?

[00:02:48.090] – Aoife Coll, Associate

So I'm going to mention two things here the first being the “Floor of Protection.” So the “Floor of Protection” is the first fundamental and basically what that means is that organisations can choose to provide a so called “Floor of Protection” so that all users get the same high level of data protection irrespective of their age. Alternatively, organisations can choose to adopt a risk based approach to verifying the age of users, so that all child users get the same high protection that's provided for in the fundamentals. The DPC do note that there will be a higher burden on internet and technology companies if they do take that risk based approach to ensure that they are protecting children with that approach. The second point then to mention relates to profiling so the DPC is clear that organisations should not profile children, engage in automated decision making in relation to them or otherwise process their personal data for the purposes of marketing or advertising, unless they can clearly show that it's in the best interests of the child while advertising. That's obviously due to the particular vulnerability and susceptibility of children to behavioural advertising. So the DPC do recognise that this will be easy to do in respect of services that are directed only to children, but it will be harder to do in mixed use internet environments.

[00:04:03.860] – Aoife Coll, Associate

And the DPC is clear that organisations in those environments, they must be able to identify and protect child users or else implement a no profiling policy across the board and it's also worth noting that the Digital Services Act prohibits advertising based on profiling by online platforms if the online platform is reasonably certain that the user is a child.

[00:04:27.880] – Aoife Mac Ardle, Senior Associate

Thanks very much Aoife. I think it's really clear from the fundamentals and from the discussion we heard earlier on that the DPC and the Online Safety Commissioner are particularly

concerned about children considering their vulnerability. So Alison, I might come to you next and I know that harmful content was mentioned a good bit in the session this morning as a new regulatory concept that might have a particular angle for children. I was wondering maybe if you could walk us through the harmful content concept as it relates specifically to children?

[00:04:59.220] – Alison Peate, Associate

Yeah, sure. Thanks Aoife, so just to kind of run through the two categories. So the first category of harmful content provided for under the Online Safety and Media Regulation Act is content relating to criminal offences. That's things like child sex abuse material, terrorist content, content likely to incite hatred, that type of thing but having a particular focus on children, I think some of the kind of more illegal content we're looking at there is relation to stalking maybe, or the sharing of intimate images which are kind of regulated under separate pieces of legislation. So I think we're all familiar with these types of content as being restricted and the sharing of it should be restricted under pre-existing legislation and then to move to the second category of harmful content, that's where it gets a bit broader and to pick up on a question raised by somebody in the audience earlier, there is that risk threshold so it's the harmful but legal content and again, just to pick up on what that target, it's things like cyberbullying, promotion of disordered eating, promotion of self-harm, suicide, that type of thing. So I think there's a clear focus there on harms relation to children in particular when you factor in the risk assessment.

[00:06:08.720] – Alison Peate, Associate

So the risk test is that the content will create a risk to the life of an individual or a significant risk to the physical or mental health of an individual, and that that risk is reasonably foreseeable. So of course, it's possible that anyone who's exposed to that type of content online, there's a risk of harm to any of us but I think we'll all acknowledge that there's a greater risk to children, given their particular vulnerability so when you factor in the risk test, I think that's where organisations will be expected to consider who's consuming the content and the particular vulnerabilities of those individuals and the risks they're exposed to. So the difference is that the first category relation to criminal offences that's automatically considered harmful content, but the second category has to meet that risk test.

[00:06:57.170] – Aoife Mac Ardle, Senior Associate

That's really interesting, Alison, and I think that risk assessment is going to be really important in terms of the enhancement of protections for children online. I was wondering, is there anything else that's coming down the tracks in terms of specific protections for children in the OSMRA?

[00:07:13.620] – Alison Peate, Associate

There's numerous explicit references to children in the Act itself. So firstly, I suppose in relation to age inappropriate content, that's something that Commissioner Hodnett focused on earlier and again, you're taking into account there the age of the individual consuming the content and whether it's appropriate for a particular age group so that's a clear focus, again, on minors. When the Commission is designating a category of content as potentially harmful, that's that second category of harmful content under the Act. The Commission is obliged under the Act to have particular regard to the interests of children and protecting children so they have to look at the type of content through the lens of a child user and whether that would be potentially harmful to a child and the Act specifies that. Similarly, they must develop online safety codes and they'll be the basis for kind of enforcing under the act and the obligations that organisations have to comply with and again, when developing those online safety codes, the Act specifies that they must consider the interests of children and protecting children in particular and just to mention, one more thing is the Youth Advisory Committee so the Commission is obliged to establish a Youth Advisory Committee within one year of the Commission having been established.

[00:08:24.790] - Alison Peate, Associate

And that Youth Advisory Committee must be made up of - half members of the committee must be no more than 25 years old. So that envisages that young people will have a direct role in supporting and advising the Commission in the exercise of the Commission's functions, to the extent that those functions relate to protecting children in particular. The DPC engage directly with children and their parents and guardians when developing those fundamentals and the same kind of concept is envisaged here that young people will inform the Commission of the types of harms that are online and what they think is appropriate in terms of obligations that should be on platforms and organisations. So I think it's clear that the focus on children and protecting children online is a key area of focus and it's not just in relation to children's privacy, it's broader than that now and it's protecting children generally online from exposure to harmful content and the risks that are posed to them and I think we can all agree that it's a really important issue.

[00:09:23.920] – Aoife Mac Ardle, Senior Associate

Thanks very much for that, Alison. I think between Aoife’s comments on the fundamentals and your comments on the new protections there, it's clear to see that a more holistic picture of the protection of children online is emerging and it's a picture that extends beyond kind of just privacy alone but it's interesting to see that both the DPC and Coimisiún na Meán are going to

benefit from the advice of Gen Z consultants as they go on this journey in developing protections. I'd like to leave children there for the minute and to go to our second kind of regulatory theme, which is going to be online advertising. I know Aoife in your comments about children earlier, you mentioned specific protections for children in relation to online advertising, but I just wanted to pick up on just the advertising aspect of that point and I was wondering if you could tell us about recent changes to the online advertising landscape and I'm thinking in particular about kind of recent regulatory decisions that touch on this space.

[00:10:17.740] – Aoife Coll, Associate

Sure. So, as you'll all be aware, the DPC released two decisions in January of this year, both relating to Meta, one relating to Instagram and one relating to Facebook. Both decisions focused on Meta's reliance on contractual necessity as the lawful basis for processing personal data in connection with targeted and behavioural advertising. So in considering contractual necessity, and in particular necessity, the DPC found that you have to have reference to the specific contract in question between the Controller and its users - here, the Facebook Terms of Use and also the Instagram Terms of Use. And also you have to have reference to the so called core function of the contract. The DPC looked at Meta's model and found that Meta's model is an advertising model so the nature of the services that are signed up to by users is funded by advertising. Therefore advertising actually goes to the fundamental object and the substance of the contract in question, which meant that Meta could rely on contractual necessity as a lawful basis for that processing.

[00:11:19.160] – Aoife Mac Ardle, Senior Associate

And when the EDPB came into the picture, did they agree with that analysis, the DPCs?

[00:11:24.900] – Aoife Coll, Associate

No, so probably no surprise there, but the European Data Protection Board did not agree with the DPC's draft conclusions in that respect. In particular, the EDPB took a kind of stricter view of the core function of the contract and they placed particular emphasis on the fact that the contract could still be performed without the processing taking place. Furthermore, they also looked at Meta's model and they said that the main purpose of the services was for users to be able to communicate with each other and the fact that Meta decided to offer its services for free to users in exchange for generating income through advertising did not mean that the processing was necessary for the actual contract. The EDPB also pointed to the right of data subjects to object to processing of their personal data for direct marketing purposes, including profiling under Article 21 of the GDPR, as supporting the conclusion that the processing could

not be necessary under the contract. So in conclusion then, the EDPB found that Meta could not rely on contractual necessity for this processing and the DPC was obliged to follow their conclusion under the Article 65 dispute resolution mechanism.

[00:12:35.890] – Aoife Mac Ardle, Senior Associate

Thanks very much for that Aoife. It's quite interesting to see how the EDPB's interpretation of the contract can have such a dramatic impact on the approach that's taken by the Controller, I might bring you into the discussion here, David, as I know you've been considering the DSA in detail for a little while now. Does the DSA deal with advertising specifically and the use of personal data for the platforms that the DSA applies to?

[00:13:00.030] – David O'Connor, Associate

Thanks Aoife. So the DSA is introducing specific restrictions on how personal data can be used for the purposes of presenting advertising online and Aoife's already mentioned one of those restrictions with respect to recipients of the service, where the online platform is aware with reasonable certainty that they're a minor. In those circumstances they'll be subject to an outright prohibition on presenting advertising based on profiling but there's also extended protections then for the rest of us, us adult recipients of the service, it's a bit of a mouthful, but for us as well, there's now a new restriction being imposed in terms of the presentation of advertisement based on profiling, which uses special category data as an input and so on the face of it, that seems relatively straightforward. But we have had that CJU decision within the past year or so which suggests that sometimes special category data can be inferred from other sources of information so it could actually be quite complex to implement this in practise.

[00:13:59.840] – Aoife Mac Ardle, Senior Associate

That's really interesting in terms of the restriction on profiling, not just in terms of the personal data of minors, but also the special category data of adults. Is there anything else coming out of the DSA that's going to affect the online advertising landscape?

[00:14:13.610] - David O'Connor, Associate

Yes, so the DSA has introduced specific rules, again for online platforms so if you're representing another type of intermediary service, they're not applicable to you. For online platforms, they're required to be more transparent with respect to their advertising and the goal of the DSA is to empower us individuals to understand when the content we're being presented with is an advertisement and once we understand that we're seeing an ad, they have provisions

in there to help us better understand why we are being targeted by that ad, in addition to who the ad is being presented by and if a different person who's paying for the ad. So maybe just to step through those four elements briefly, in terms of better understanding that the information you're seeing is an ad, individuals should be able to identify in a clear, concise, ambiguous, we all know this sort of language from GDPR, manner and in real time that the information is an advertisement and that will be achieved primarily through the use of prominent markings and then once we understand that we're seeing an ad, online platforms will be required to provide us with information directly from the ad, which will allow us to better understand the main parameters that were used to target us and where applicable, how we can influence those parameters in the future.

[00:15:29.540] - David O'Connor, Associate

And so when we understand that we're seeing an ad and why we're seeing it, we should also have information on whose behalf the ad is being presented for/ by. So I think that's in the vast majority of cases be pretty straightforward. You see your ad for Cornflakes, you know, it's Kellogg's but I think on social issues, I think that would be pretty interesting, where there might not be such a clear connection between the person presenting the advertisement and the message itself and so that's where the final element kicks in in terms of providing information on who is paying for the ad and I think, you know, again, on those social issues and political issues, advertising that area is going to be a really effective tool for improving transparency.

[00:16:09.010] – Aoife Mac Ardle, Senior Associate

That's really interesting, David. In the new world of the DSA, we're going to get to learn a lot more about what we're seeing online, why we're seeing it, and also who's paying for us to see it. Just thinking of kind of another element of how things are promoted online and thinking about user generated or influencer content. Is there anything in the DSA that speaks to that kind of element of online promotion?

[00:16:32.190] - David O'Connor, Associate

Yes, there is. So again, it's rules that apply to online platforms specifically, and the goal here is quite similar. It's that we should understand when we're seeing sponsored content. So obviously the online platform, it has no way of knowing when information is uploaded that it is an ad but what they are required to do is to facilitate individuals to declare that the content they're adding to the platform is or contains commercial communications and then once the online platform has that declaration, then they can make sure, through the use of prominent markings, that we as individuals can see that we're dealing with sponsored content here.

[00:17:08.340] – Aoife Mac Ardle, Senior Associate

I'm conscious that there's quite a lot of regulation that's coming for VLOPs and VLOSEs specifically so is there anything specific for them in this kind of advertising transparency space?

[00:17:17.690] - David O'Connor, Associate

Yeah, there is. So for those VLOPs and VLOSEs, so again, those with 45 million monthly active recipients or more, they're required now to put in place a repository of online advertising and the repository I think would be really interesting. It's required to store information on all the ads that were presented by the VLOP or VLOSE within the last twelve months in addition to all the ads that are currently being presented on the platform. The repository will have to store the content of the ad itself so we'll have a record of what was presented. It will have to include all the information I've discussed in terms of on whose behalf is the ad been presented and who was paying for it, but it will then also have to include other information, such as the performance and reach of the ad. So on a member state by member state basis, the repository will have to set out how many people were exposed to the ad, and specifically for the group of individuals who were targeted, whatever their personal characteristics were. The repository will also have to provide information on how many of those were presented with the ad.

[00:18:17.700] – Aoife Mac Ardle, Senior Associate

Thanks, David. It's really interesting how transparency is such a driver for all of those requirements that we're seeing kind of across all of the different entities that are regulated by the DSA, just to keep that transparency theme going, but maybe go in a little bit of a darker direction, Alison, I might come to you on the topic of dark patterns. It's something that we've heard a good bit about in the GDPR context behaviours that maybe try and nudge certain reactions from online users and I know that there's specific regulation coming for them in the DSA, so I was wondering if you could maybe unpack that dark patterns concept a little bit for us.

[00:18:52.350] – Alison Peate, Associate

Yeah, sure. Thanks Aoife. So, as you said, I think dark patterns and deceptive patterns, whatever you want to call them, they're concepts that we're familiar with from existing data protection law and consumer protection law as well but they're now regulated under the DSA, so it makes the situation a bit more complex in terms of "what piece of legislation do you fall under?" I might just begin by kind of setting out what we mean when we say dark patterns and have a look at kind of the context that we're used to seeing the dark patterns come up in. So

there's no one definition of dark patterns across all of these pieces of legislation, but it gets at any kind of practise that manipulates or deceives an individual and kind of nudges them, like you said, to make a choice that they wouldn't have otherwise made, in particular if that choice has a negative impact on the individual. So the GDPR and the E-privacy Directive and Consumer Protection Law do form part of the current legal framework that regulate the use of dark patterns, but they don't explicitly refer or prohibit dark patterns but I suppose the context that we're used to this coming up in the context of GDPR at least, is in relation to consent.

[00:20:03.290] - Alison Peate, Associate

So if an organisation is looking to rely on consent as a legal basis for processing data under the GDPR, or looking to get consent to cookies for the purposes of advertising, if an organisation presents that choice to a user in a way that kind of gives promotion to the opt in option, or makes it very difficult to change the default settings, that could be a dark pattern because the information wasn't presented in a neutral way and as a result of that, the consent that the organisation tried to get might be invalid because it wasn't freely given, it wasn't informed and it didn't comply with the Article Five Principles in the GDPR on Fairness and Transparency, like David mentioned as well so that's the context that we're used to seeing dark patterns being regulated at the moment.

[00:20:51.420] – Aoife Mac Ardle, Senior Associate

And how are dark patterns going to be regulated under the DSA?

[00:20:55.400] - Alison Peate, Associate

So under the DSA, there's an explicit prohibition on the use of deceptive patterns in a way that makes the user make a choice they wouldn't have otherwise made and I think that's helpful in one sense, because it does make the prohibition explicit. So it's gone further in a way than what we've seen under the GDPR and Consumer Protection Law but the kind of caveat to that, I suppose, is that the prohibition in the DSA says that it won't apply to practises that otherwise fall within the scope of the GDPR or existing consumer protection law. So that begs the question then, of what is left for the DSA to catch? And as you know, I've spent some time thinking about this and I don't have a perfect answer to it, and I think all that immediately comes to mind for me is kind of business to business relations that would be caught because they're not otherwise caught by consumer protection law. So on the one hand, I think it's a bit of an unsatisfactory position because I think the GDPR and consumer protection law haven't been particularly successful at preventing the widespread use of dark patterns.

[00:22:02.390] - Alison Peate, Associate

So by giving primacy to the GDPR and Consumer Protection law in the DSA, it begs the question of what effect the prohibition in the DSA will actually have. On the other hand, like I said, I do think it's helpful that the prohibition is explicit this time. It does clarify the legislative intent around dark patterns so I think, not that it was ever in doubt that these things are not allowed, that's made clear now and I think instead of maybe getting bogged down like I did in the legal or academic discussion about what the DSA will catch, it probably is better for organisations to take a practical approach and just focus on preventing these types of practises and patterns on your user interfaces and present material in a way that's neutral and don't promote one choice over another. So regardless of what piece of legislation it might fall under, I think the intent is clear that it shouldn't be done. So to come back to David's piece on transparency, transparency is a key concept that we're familiar with, obviously, under GDPR, it's also a key concept in the DSA, so transparency is key and that relates to dark patterns and also fairness under the Article Five in the GDPR and under Consumer Protection Law.

[00:23:20.020] - Alison Peate, Associate

So I think that should be the focus, rather than getting lost in the theoretical thought process that I did.

[00:23:25.880] – Aoife Mac Ardle, Senior Associate

Thanks, Alison. So, from a legislative drafting perspective, it's not exactly the ‘Empire Strikes Back’, but some practical guidance for people there in terms of the intent of that prohibition. So I know we've been discussing regulatory themes around children and online advertising, which have traditionally been hot topics under Data Protection Law, but I think now we'll move to our third regulatory theme here and it's going to be operational compliance under the DSA. Lorraine, I might turn to you and bring you into the discussion here as I know you've been thinking about the new obligations that are going to be on different entities that are caught by the DSA and how entities and I'm sure many of the people in the room can give operational effect to a lot of these obligations. Can you talk to us a little bit about the compliance framework that's coming?

[00:24:13.540] – Lorraine Sheridan, Associate

Yeah, thanks Aoife. So, there's no doubt that there are going to be increased compliance obligations coming on organisations on the back of the DSA. So people have called out some of the obligations already, Dave has gone through a lot of the obligations around advertising so I think it might be helpful to look at the inverted pyramid of compliance. So if we look here, so at

the bottom we have all intermediary services, then we have the hosting services, online platforms, and then VLOPs and VLOSEs at the top. So the nature and the breadth of your obligations will increase as you go up that pyramid. Now, I will just say that the VLOSEs are slightly different in terms of the cumulative nature, but for the most part we're talking about if all intermediary services have some obligations, then if you're hosting service provider and above, you have additional and that's kind of how it works. So, so far the designation of VLOPs and VLOSEs, so there's only been 19 designated by the commission so far. So we're only talking about 19 entities at the moment. At the top so it might make sense to start at the bottom and talk about the compliance obligations from the bottom up.

[00:25:15.800] – Aoife Mac Ardle, Senior Associate

So at the bottom of this pyramid, we're basically looking at the largest number of entities that will be affected, but the smallest number of obligations and as we climb the pyramid, we get smaller in terms of entities, but bigger in terms of obligations and that's what you can see at the top of that inverted pyramid there, is that right?

[00:25:33.480] - Lorraine Sheridan, Associate

Yeah, exactly. I might call out three of the obligations that apply to all intermediary service providers. So we're at the very bottom, so the first is the appointing a single point of contact so all intermediary services will have to appoint single points of contact to deal with the Commission, to deal with the European Board and to deal with member state authorities, and also to deal with the service recipients directly and the obligation is to deal with them rapidly. So that's something that they'll have to do. Additionally, a concept we'll be familiar with under the GDPR is if you don't have an establishment in the EU, but you offer your services in the Union, you'll have to appoint a legal representative. And I suppose the one difference with the legal representative that needs to be appointed under the DSA is that they will be personally liable for infringements of the DSA by the organisation, because I think the GDPR was a little bit unclear on that point.

[00:26:22.150] - Lorraine Sheridan, Associate

The second thing to talk about is the terms and conditions. So all intermediary services must describe their content moderation practises, the procedures they use, the tools they use, and also, if the services primarily are predominantly directed at children, those terms will have to be understandable and they'll have to set out any conditions or restrictions on the use of those services by children. Now, as you go up the pyramid, the VLOPs will have additional obligations when it comes to what's in their terms and conditions but the obligation to have the terms

conditions is universal and I suppose the third thing to talk about then is transparency reporting. So this is where the content moderation activities that the organisation undertakes, they should be produced at least annually. They'll touch on things like the number of complaints that the organisation has handled, what automated means that they use, and the notifications that they've or the notices they've received to act on illegal content. Again, the frequency and the content of those reports changes as you go up the pyramid but the obligation to produce the reports is universal.

[00:27:22.370] – Aoife Mac Ardle, Senior Associate

Okay. So the universal building blocks at the bottom of our pyramid, we have our points of contact or legal representatives, terms and conditions in respect of content moderation and then the transparency reporting. So if you take us up a level on the pyramid, Lorraine, what are we looking at there?

[00:27:37.970] - Lorraine Sheridan, Associate

So if we go to hosting services then. I was referring to earlier the notice and takedown mechanisms so if you're a hosting service, and online platform or VLOP, you'll need to have an easily accessible way that individuals can notify you of illegal content on the platform and you also have to have processes in place to deal with those notices in a timely, diligent, objective and non-arbitrary manner. There's also an obligation to produce statements of reasons. So if you're going to remove illegal content or restrict service recipients, you'll have to produce a statement of reasons setting out how you came to that decision. So these are things that organisations will have to look at resourcing in the background.

[00:28:12.680] - Aoife Mac Ardle, Senior Associate

So your next level of the pyramid, we have your notice and takedown regime is a key obligation there. So if you take us up a level again, Lorraine, what do we see?

[00:28:23.140] - Lorraine Sheridan, Associate

So, if we go up again, we're looking at things like complaint and redress mechanisms. So under the DSA, users will have new rights in relation to availing of internal complaints mechanisms, seeking out of court settlements and seeking compensation for infringements of the DSA. So online platforms and VLOPs will need to ensure that they have sufficient measures in place to operationalise those. The other thing is that if your platform allows for the conclusion of contracts between traders and consumers, they'll have obligations as regards Trader

Traceability so this means that platforms will have to collect certain information in relation to their traders and assess that and analyse that information and they'll also have to keep that information for a certain period of time after the conclusion of their relationship with that trader. So the kind of emphasis there on ensuring that illegal or counterfeit products aren't sold online, for example, is kind of one of the things that's getting at and kind of enhancing consumer protection in that way.

[00:29:15.480] - Aoife Mac Ardle, Senior Associate

Okay, so compliance obligations here, they're getting a bit more onerous in terms of what needs to be done to implement that redress mechanism and the Trader Traceability Programme you outlined there. Dare I ask you to take us up another level to the top of the pyramid now?

[00:29:28.770] - Lorraine Sheridan, Associate

Yeah. So if we go to the top, then we're talking about those 19 entities that have been designated so far and they'll have to do things like prepare risk assessments, conduct annual audits and also to establish a compliance function and I think the establishment of the compliance function has been something that's kind of been covered a lot in the commentary about the DSA. So the risk assessments, what organisations have to do is they have to identify and analyse the risks that are associated with the functioning and use of their platforms. So the DSA does set out some specific risks that need to be addressed, such as the dissemination of illegal content and any foreseeable negative effects that would have on the protection of public health or the protection of minors. As we talked about earlier, they'll have to be produced at least annually then the annual and independent audits are audits for the VLOPs compliance with their due diligence obligations under the DSA, but also any commitments that they've made under codes of conduct or crises protocols and then the establishment of the compliance function. So it's kind of similar to how, I suppose, the DPO is under the GDPR, we have to have an independent kind of compliance function.

[00:30:28.880] - Lorraine Sheridan, Associate

They'll be the people that will be assisting with the risk assessments and monitoring the organisation's compliance with the DSA. Similar to the GPO, they have to have certain qualifications, they have to have certain experience in order to carry out that role. So there are obviously more obligations on VLOPs and VLOSEs as well, but they're some of the key ones. So I guess to circle back at the bottom of the pyramid, we have these universal obligations and then as the number of users of these platforms will generally ascend as you ascend the pyramid as well. So that's kind of how it works with building blocks.

[00:31:01.100] – Aoife Mac Ardle, Senior Associate

Thanks very much for that, Lorraine. I think that pyramid structure with large number of entities, small number of obligations, inverted top with large numbers of obligations and small numbers of entities, I think that paints a really clear picture in terms of how the compliance framework is going to work. I might bring you back into the discussion now, David, as I know you've been thinking about kind of the back office or the engineering aspect of a lot of the obligations Lorraine took us through on the pyramid there. What are some of the big technical lists that you've identified in your review of the DSA?

[00:31:32.190] - David O'Connor, Associate

Thanks Aoife. Yeah, so I suppose it's a corollary of what Lorraine has just talked us through. Depending on the type of intermediary service you provide, the fewer obligations you have, the easier your technical lifts should be. So if you're exclusively at the bottom of that pyramid, you're providing mere conduit services or caching services. Thankfully you should have, hopefully a relatively easy implementation as you move on then to hosting service providers. Still, some of it is quite good news from a DSA perspective. I mean, this is an evolution on an existing liability framework regime that has existed since the early 2000s under the E-commerce Directive, so you might already have systems in place. So it's about looking at some of the changes in the DSA and thinking, how does that help me in my current operations, particularly on the legal op side of things. So, for example, those notices of illegal content, they're now required to be submitted via electronic form. So hopefully that will free you from dealing with sort of traditional snail mail, which hand typing up URLs and so on and then also the DSA has put on a statutory footing minimum information requirements, without which the notice is not valid.

[00:32:40.010] - David O'Connor, Associate

So again, if you think about your existing machinery that you have in place to comply with your e commerce obligations and think how you can rework it. On the front end, you could revise your web forms and think, how can we change this in light of the minimum information requirements set out into the DSA to raise the quality of the notices we're receiving. You can think about in terms of how can you operationalise this statement of reasons obligation that Lorraine spoke about, explaining to users why we've deleted your content, why are we demonetising your account, why are we placing some other restrictions on your account? You can start to think, how can your existing machinery be amended tweaked so that you can churn out in an automated fashion or semi-automated fashion these communications to users translated into all the different EU languages that you'll need to cater for. So for the hosting service providers, I

think it's not all bad news and there'd be technical investments, but it should improve operational efficiency as well.

[00:33:42.410] – Aoife Mac Ardle, Senior Associate

Thanks, David. That's really helpful pointing out the overlap between e-commerce obligations and the DSA obligations for the hosting services providers, I'm thinking what are some of the other obligations if we go up a level on the pyramids, the online platforms that apply to them? I'm thinking in particular some of the obligations around the appeals mechanism that Lorraine mentioned.

[00:34:02.510] - David O'Connor, Associate

Yeah. So exactly. Again, it'll be more evolution rather than revolution for some of these online platforms but I think this internal complaints procedure is really interesting because what it's doing is it's putting on a statutory footing now an appeals mechanism for individual recipients of the service. So we've always been able to appeal a decision to remove content or to restrict or suspend our account, whatever it may have been but what the DSA has now done by establishing this internal complaints mechanism, it is now requiring online platforms to enable and facilitate the submission of sufficiently precise and adequately substantiated complaints and it's a bit of a fudge, on the one side we've concise to the point, on the other side we have adequately substantiated and what is that actually going to mean in practise? But if I were an online platform, what I would be doing is reviewing my current appeals mechanism and I'd be looking at what restrictions are we placing on our users when they're trying to appeal a decision? So are we forcing them to use a limited number of prescribed drop down options? Are we imposing quite low character limits in terms of how much information they can provide us?

[00:35:17.480] - David O'Connor, Associate

Are we restricting them from providing attachments? And again, there are really good operational efficiency reasons why you would have a streamlined system in place but I think, given that this appeals process is now in a statutory footing, you should look at these with fresh eyes and consider what amendments might be appropriate.

[00:35:35.140] – Aoife Mac Ardle, Senior Associate

So online platforms could be better off in the long run to beef up their internal appeals procedure and allow for longer but concise submissions.

[00:35:46.340] - David O'Connor, Associate

There's also now a statutory multistage appeals process so you've got your out of court dispute planes handling procedure, but if you don't like the outcome of that, you also now will have recourse to out of court dispute settlement processes. So again, it will depend on user by user the nature of the complaint but it could be, as you said, better off in the short term, allowing for more lengthy submissions when you're considering whether your initial decision was correct and there's so many other I think in the interest of time, we probably have to gloss over them but even I mentioned earlier the transparency rules around online advertising. To provide all that information directly from the ad itself will require an investment and changes and overhaul to the user interface of these platforms across laptops, mobile, tablets, across all these surfaces. And that's no small matter. So even those seemingly easy requirements could be large technical lifts for the online platforms.

[00:36:42.090] – Aoife Mac Ardle, Senior Associate

So the engineering work that's required is kind of really starting to stack up there and I'm conscious that we haven't even mentioned the very large online platforms or very large online search engines. In the interest of time, are there a couple of key aspects of the technical lift that they'll have to implement that you could call out?

[00:36:59.240] - David O'Connor, Associate

Yeah, of course. I think, again, for time reasons, it makes sense just to look at those marquee obligations around risk assessment and putting in place those mitigation measures. So bearing in mind these are the intermediaries with 45 million plus users throughout the European Union, the machinery that would be required to monitor and identify and assess risk at that scale across all the different areas that are set out in Article 34, from consumer protection to child protection to data protection. That itself will be a massive undertaking and will be underpinned, I'm sure, by dozens or possibly hundreds of people who are working hard on these topics right now. And then for the mitigations, each and every mitigation could be an engineering project in its own right, especially considering that it will be subject to external independent audit. So I think from a technical perspective and a personnel perspective, we're looking at years of investment.

[00:37:57.040] - Aoife Mac Ardle, Senior Associate

Thanks for giving us that perspective on the technical work that's required to support these obligations, David, it's a very lengthy to do list and I don't know that I've had a to do list that's lasted for years, but it seems like that's what's facing many of the entities regulated by the DSA.

Before we finish up our panel today, I want to come back to you, Lorraine. I know you set out for us earlier the inverted pyramid and how it's going to affect different entities and David's just put that into three dimensions there by describing all the technical work that's needed to support those obligations. I suppose for anyone that's worried about having a year's long to do list, is there anything you've identified from the DSA that maybe overlaps with compliance steps that organisations may have taken for the purposes of the GDPR?

[00:38:41.430] – Lorraine Sheridan, Associate

Yeah, sure. So I think the DSA has all these new obligations and compliance officers are understandably overwhelmed with the amount of new obligations that are coming down the track and I guess not only under the DSA, but under all of the legislation that Olivia mentioned earlier and then some. So I think it's important to take a step back and take stock of the compliance work that's been done within your organisation, particularly over the last five years, in order to comply with the GDPR, but also under numerous other pieces of legislation. So I think one thing to look at is transparency reports. So transparency reports are kind of industry best practise at the moment and what the DSA has done is put the obligation to produce those transparency reports on a statutory footing. So the DSA sets know what needs to be included in those reports, but there is also scope for the Commission to produce forms, guidance and templates for those reports. So I think we could have a situation a bit like privacy policies in the GDPR. So we all thought when we were drafting these policies in 2017/2018 that we were complying with Article 13 and 14.

[00:39:47.030] - Lorraine Sheridan, Associate

So therefore we had a compliant policy and it wasn't really until the WhatsApp decision in 2021 in relation to their privacy policy that we actually realised that the regulatory expectation is a little bit higher and we got more detail. So I think the nature of these transparency reports might develop as the DSA beds in, but it is reminiscent of kind of the industry best Practise as it is.

[00:40:08.610] – Aoife Mac Ardle, Senior Associate

Okay, so some maybe room for evolution and bedding in as this kind of concept in the DSA framework really kind of gets embedded. One of the things that strikes me is we heard a bit even in the panel earlier about risk assessments and audits. Is there any kind of overlap with existing GDPR compliance with those?

[00:40:25.770] - Lorraine Sheridan, Associate

Yeah, sure. So risk assessments are not dissimilar to the data protection impact assessments that we would prepare where the processing is likely to present a high risk to the rights and freedoms of table subjects. So in a DPIA, we look at the processing, we look at the risks and then we seek to apply mitigations to lower to mitigate that risk. So I think under risk assessments, that's essentially exactly what we'll be doing. The DSA is prescriptive and they must be conducted annually. So I think it's definitely something that you don't want to leave on the long finger between these risk assessments as soon as we can. The other thing to mention with the risk assessments is that the supporting documentation needs to be kept for three years and we produced on request. So still something for organisations to keep in mind when they are actually doing their risk assessments and then on the audit piece. So under the GDPR, there was no legal obligation to conduct an audit for your compliance with GDPR, although lots of organisations are doing so and we'll be used to doing compliance audits for security compliance and different things like that.

[00:41:29.120] - Lorraine Sheridan, Associate

So hopefully it's just a matter of plug and play that your statutory obligation to conduct your audits under the DSA, if you're a VLOP, can just be added to your yearly compliance audits anyway.

[00:41:40.340] - Aoife Mac Ardle, Senior Associate

Thanks very much for that, Lorraine. So some overlap with things organisations are doing at the moment, but kind of an enhancement in terms of everything that they have to consider and I know, as Rob mentioned earlier, be fascinating to see the results of that process in a year's time. So I think we're nearly out of time for this panel. And just to sum up some of the key themes from the discussion today, it seems like we're moving towards enhanced protection in areas that we've seen before, like protecting children and online advertising but that the level of work. That's going to go into supporting all of these new obligations is quite significant, albeit that there may be some areas of overlap with common themes that organisations are tackling at the moment. I'd like to say thanks very much to our panellists, to Aoife, Alison, David and Lorraine for sharing all of their insights with us this morning.