

Learning outcomes: 1. Why good CASS governance and oversight matter 2. GDPR: what it is and who it affects 3. MiFID II and how prepared firms are to address it

**PRESENTER:** Regulatory change can be a headache for those in the financial industry, especially with MiFID II just around the corner. So what do financial professionals need to be aware of, and what technological solutions are available to help? In this Akademia unit, we're going to be looking in more detail at this issue. On the panel are Gill Boston, Head of Business Consulting for AutoRek; Anastasia Georgiou, Product Manager and Advisor Software for Morningstar, and Jonathan Wright, Solicitor for Wedlake Bell LLP. There are three key learning outcomes. Why good CASS governance and oversight matters. We'll also examine GDPR, what it is and who it affects. And we'll look at MiFID II and how prepared firms are to address it. Anastasia, let's start with the latest regulatory developments that are impacting the investment management space. What would you say they are, and how are they going to really impact advisers?

**ANASTASIA GEORGIOU:** Well, there's a lot of regulation going on right now. There's the PRIIP, which is new reporting regulation. There's GDPR which I know we're going to talk about a bit later. There's PSD II, which is payments ex-directive, but it's going to force the banks to open up their digital doors, and make consumer banking information available to third parties if the consumer so wishes. And then I think one of the biggest issues that the industry is facing is MiFID II. So that's probably the biggest impact right now that everybody's focused on. It's a really wide reaching regulation, and it's impacting both distributors and manufacturers. It's primarily focused on investor protection and market stability, and brings in new rules around product governance, disclosures and suitability.

**PRESENTER:** And Gill, from a data management perspective, what sort of things are you seeing?

**GILLIAN BOSTON:** I think generally speaking there's so much regulation as Anastasia has already said there, and it's not going to go away and firms really need to think about how long term they have efficient and effective solutions in place to do so. We still see a lot of firms who have very manual processes, and go so far and then use spreadsheets as part of their control regime. So it's really about firms having to think about the sustainability and the maintainability as regulation changes and indeed their businesses grow.

**PRESENTER:** Well we're going to talk more about CASS compliance and MiFID II a little bit later on, but first Jon Wright is going to join us in the studio to discuss GDPR. Well, Jon, as we heard there's a lot of regulation that's impacting the investment space. What would you say are the top three issues?

**JONATHAN WRIGHT:** The top three issues on the GDPR, the General Data Protection Regulation, is the fact that it's just brought data protection to the forefront for many investors and organisations as well. So before it kind of sat in the background, but the eye-watering finds which have been thrown around has really brought it to board attention. So they've freed up space and the infrastructure required for actually a data protection compliance moving forward. And with the advent of all of these data breaches, it's really brought it to the public's attention, so people expect their data to be protected. So it's actually a way for investors to choose who they're advised by. And there was a recent survey that said 82% of investors would reconsider using or not use an adviser that suffered a data breach. So it's organisations' best interests to become compliant. And it's changed the way in which they interact with their investors as well. So the information they provide they have to be more transparent. So they have to tell them exactly what their data is being used for, and they have to get their opt-in consent if they want to send them marketing information about new opportunities, for example. And generally the way they share data with financial institutions, they need to have the appropriate agreements in place, which can be quite a time consuming job.

**PRESENTER:** Well it seems like a very simple question, but what exactly is GDPR?

**JONATHAN WRIGHT:** Well it stands for General Data Protection Regulation, and it's the new European-wide regulation which replaces the Data Protection Act in the UK, and it's all about the processing of personal data.

**PRESENTER:** And who does it apply to, and what information does it apply to?

**JONATHAN WRIGHT:** Well as I said it applies to the processing of personal data. And personal data is any information by which a living individual can be identified. So it's a name, a photo, it

can be your location, your ISP address, just your telephone number, anything like that that can be used to identify you. PRESENTER: So, the existing data protection law, this has been around about 20 years, so what sort of differences are we looking at when it comes to GDPR? JONATHAN WRIGHT: Data Protection Act 1998 actually started being drafted in the 1980s, so it's before the advent of the internet and connected devices, smartphones, tablets, the user generated content on social media. So you can think how far we've come in the space of 20 years. The Data Protection Act is totally out-of-date, and it's amazing it lasted as long as it did. So there's all these calls for reform, and there's been a lot of changes introduced by the General Data Protection Regulation, the GDPR; most notably the requirement for accountability for organisations, so you need to be able to demonstrate compliance. So you can't just say you're compliant, you need to have policies, procedures in place, and you need to be able to prove that you're taking the steps required. There's changes to breach notification. It's mandatory. So if you suffer a breach you have to tell the supervisory authority, which is the ICO in the UK. And in some circumstances you have to tell your investors. So the data subject, you have to tell them what's happened and what data has been lost or what's been stolen, for example. There's requirement for mandatory data protection officers. So if you process a large volume of sensitive personal data. So things about health, nationality, that kind of thing, you have to have a data protection officer - which will apply to a lot of financial institutions, especially due to the volume of information that they process - and then it's a case of finding the right person that has the right qualifications, and that's not always easy. There's changes around the penalties, which I've spoken about, the eye-watering penalties, so it's €20m or 4% of global worldwide annual turnover, whichever's greater, and there's other penalties, which I'm sure we'll get to. There's changes around consent. So to process personal data you need a justifying ground, and the most common one which people tend to focus on is consent. So for consent to be valid under the GDPR it needs to be freely given, unambiguous and for a specified purpose, and you need to have documented evidence. So this impacts marketing and how you approach your investors and get their consent to send the marketing. You can't rely on consent with your own employees, or it's very difficult to, because employee consent isn't seen as being freely given due to the balance in the power. So the employee may fear giving consent to their employer so you can't be freely given from that perspective. But there's a whole host of other ones as well, so I don't want to bore everyone, so I'll stop there. PRESENTER: So a lot of changes afoot then. JONATHAN WRIGHT: A lot of changes, yes. PRESENTER: But we're in a transition period here in the UK, so how will Brexit impact this regulation? JONATHAN WRIGHT: Well I think this has now been nailed, done and dusted now. I think there are a few hopeful people that stood their head in the sand and thought Brexit, it's not going to apply; it's a European regulation. But I think now that's been addressed. So the Information Commissioner has said that Brexit won't mean Brexit for data protection standards. And also we'll be in Europe, we'll still be in the EU come the 25th May 2018 when the GDPR comes into force, so it will apply, it's coming. What happens post Brexit is another thing. But there's an extended scope with the GDPR. So even if you're outside of Europe or the EU, and you want to sell your, you want to target customers inside the EU, then you still have to comply the GDPR. So if your investors are, if we're outside of the EU and your investors are inside the EU, then you still need to comply with the GDPR. And also when you're outside of Europe or the EU, you're considered to be a third country for the purposes of the General Data Protection Regulation, and transferring data to third countries is quite difficult. And you have to prove adequacy so that your standards of data protection mirror or are adequate to those inside the EU. And one way of doing that, and the easiest way of doing that is to adopt a similar or same kind of protections that are put in place by the GDPR. So, when we leave, it might not be called the GDPR, but the standards are most likely to be very similar. PRESENTER: Now, there are probably people out there who haven't even heard of this regulation, so what are the penalties for non-compliance? JONATHAN WRIGHT: So, the penalties, I've mentioned some which are this 4% of worldwide annual turnover of €20m, which are eye watering. And

to be put it in perspective under the Data Protection Act the maximum fine was £1/2m. And there weren't ever any fines of £1/2m but TalkTalk were fined £400,000, and the equivalent amount under the GDPR would be over £71m. So you can see there's a huge increase. But, in addition to these eye-watering fines, there's the ability for compulsory audits. So the ISO or the supervisory authority can turn up and audit your systems to make sure that you're being compliant. And they can actually freeze your processing activities. And many businesses rely on processing and sending personal data, so if they stop you doing that your business effectively shuts down, which can be very costly. You can't meet customer demand, you can't do anything essentially. And there's also this new private right of action for misuse of personal data. So individuals can now bring claims against organisations that have misused their personal data. I think the sums you're talking about there are quite small. But if for instance you have a data breach which involves 50,000 individuals, then those small amounts will add up to something quite substantial. PRESENTER: So the most important question I think for most people is how can they prepare for it and when's the deadline? JONATHAN WRIGHT: So the deadline, it's coming on the 25th May 2018. So come the 25th May you need to be compliant; otherwise you're at risk. So you've got some time but six or seven months isn't a long time when you realise how much personal data you hold as an organisation, especially as financial advisers or financial organisations. But one of the key things to do first before you can comply, you need to know exactly what personal data you hold. So you need to audit your systems and find out what information you have. Is it employee information, do you have investor information, what other personal data? To get in the building today I had to sign an entry/exit log, and that's my personal data putting my name down there. So you need to know what you have. So you need to conduct a data protection audit. Secondly, once you find out what you have, you need to find out where it goes. So who you send it to, which financial institutions do you send it to? Do you use various service providers, do you have an outsourced HR system like Workday that centralises your HR systems. So who are you sending your information to? So it's known as dataflow mapping. And then once you've done that you need to make sure you have the policies and procedures in place that show that you're accountable for that data, that everyone knows what they should be doing with it. There's policies and procedures and place to do with security. Everyone's been sufficiently trained, so all your staff know what personal data is and what they're supposed to be doing with it. They don't need to be experts, they just need to know what they need to do with personal data, so you need to have training in place, and everything needs to be documented. And another key change, which I should have mentioned earlier, was this idea of a privacy impact, a data protection impact assessment. So, if you're going to conduct a new marketing campaign to target new investors, something which will involve a risk to data subjects or involve personal data, you need to, it's like a risk assessment that you undertake at the outset. So you take personal data and protection of personal data into consideration at the beginning. So you kind of bake it into the process at the start, rather than just tag it on at the end once you've decided what you're going to do. So if you were going to launch a new piece of software, a new CRM system, or a new way that your investors can log on and interact with you, you would have to run a data protection impact assessment, document the decisions, what risks they are, how you've mitigated them, why you've decided to take a risk-based approach and accept that risk. Because if there is a data breach, the first thing the supervisory authority will ask you is did you conduct a data protection impact assessment? And if the answer is no, then you're on the back foot from the outset. PRESENTER: Jon, thank you. JONATHAN WRIGHT: No problem. PRESENTER: Well, as we heard from Jon, there's certainly a lot of changes afoot. So now let's move on to CASS compliance. So, Gill, looking at the new regime for CASS audits, what's the ramifications; there seems to be a lot of mixed opinions there? GILLIAN BOSTON: Mixed opinions, yes. Well I suppose what we're seeing is, as I already mentioned, the whole data management piece. Firms have actually spoken to us in the past whereby they've had trouble or had difficulty securing budget for regulatory projects. So I think with the new, or rather enhance audit

regime with the senior managers regime, which I'm sure we'll touch on shortly, I do think that actually regulatory projects with respect to CASS, and also the adverse opinions that we're seeing coming out of the revised audits if you like, I think that's actually helping firms think about how can you do things more efficiently and effectively, because it's not going to go away, anything but. So hopefully the ramifications are still a bit of a pain for firms to work and ensure they have the right controls and the right transparency and governance of data that they need for CASS, but hopefully the senior managers regime, the enhanced audits will actually turn out to be a good thing. PRESENTER: And how important are centralised processes and robust controlled frameworks? GILLIAN BOSTON: Very, I mean they absolutely are because at the end of the day the FCA want to really see firms drive up client protection, so I would say they're fundamental. PRESENTER: So auditors, regulatory breaches, I mean what's the best way to manage these? GILLIAN BOSTON: I think what you need to do and the best way to manage them is truly understand why those breaches or those errors have occurred. It's almost like an education, really understand why they've happened, make sure they're not going to happen again. The FCA won't take kindly to seeing the same type of mistakes or errors or breaches coming through. I suppose at the end of the day it's about culture and behaviours as well within firms. It's really so people who work with CASS, so many people it touches on their day-to-day jobs. So it's really an education in terms of understanding what you do, why you do it, but in particular the ramifications if it does go wrong. PRESENTER: So good CASS governance and oversight, it really does matter. GILLIAN BOSTON: Again absolutely fundamental yes. PRESENTER: So now let's move on to MiFID II that's causing a lot of waves in the industry at the moment. So, Gillian, why now and how ready would you say firms are actually to address this? GILLIAN BOSTON: I would say firms are perhaps not as ready as they should be. I think that's fair comment. Interestingly there was a speech given by the Enforcement and Market Abuse Director from the FCA just recently. He's indicated that investigations are on the increase, and went on further to say that I don't think the FCA will take very likely to firms that aren't compliant with MiFID II from the 3rd of Jan 2018. Because at the end of the day it was postponed for a year, so I think there's still quite a bit of work to be done. PRESENTER: And Anastasia, what kind of changes can we expect? ANASTASIA GEORGIU: Well, for financial advisers, there's a number of changes they need to make. I think the UK financial adviser having been through the RDR has already got a lot of the processes in place, and has taken steps already to be somewhat MiFID compliant. So we've already got independent advisers being fee based. Advisers already have a suitability process in place. The levels of training and competence probably are good enough in the UK. But there is still work to do. So for example on the advice process in terms of suitability, advisers are going to have to have a process in place to do at least an annual suitability assessment, and they're going to have to have processes in place in instances where they can't get hold of their clients to do that, they need to be able to mitigate against that. There's also some changes around the definition of independence. So any UK adviser that is already compliant with the RDR definition of independence is fine, but being independent will mean that you can advise on a segment of the market. So for example an adviser can be independent and just advise on a segment of the market. So for example they could just advise on funds, as long as that universe was far reaching and wide enough. And also advisers will be able to be both independent and restricted as long as they don't call themselves independent, and they have separated out the services. So it's not the adviser giving the restricted and the independent advice. PRESENTER: But I imagine, like with most new regulation, there are different interpretations. Would you say this raises issues? ANASTASIA GEORGIU: Yes, I mean there's definitely different interpretations. I think the way to deal with it is really to see the regulators that industry bodies and associations and industry coming together to work through those changes and take a practical approach to taking the regulation and making it something that's workable. And I think we've seen that happening with MiFID II. So we've been involved in a number of working groups looking at different streams and coming up with

best practice approaches. PRESENTER: So how ready are advisers, and what's the common misunderstandings then and mistakes they're likely to make? ANASTASIA GEORGIU: So I think as Gill said, I don't think, well, the advisers are as ready as they should be or they could be. We actually did a survey ourselves at the beginning of the year, and we found that in the space of asset management and banks, those groups were very aware of what needed to be done, and were at least in the process of looking at all the different streams and impacts. With the financial advisers, there was, you know, it was quite a contrast. They didn't really see the impact yet. And even yesterday actually we ran an event, and we had about 30 financial advisers attend, and not one of them felt they were ready, and of that group only a third were ready to at least be processing and reviewing what they needed to do. So there's still a lot of work to be done, and a lot for advisers to get their heads around. PRESENTER: Well like I asked Jon, I mean we're in this uncertain period of Brexit negotiations, do you think Brexit will have much of an impact on MiFID II? ANASTASIA GEORGIU: I don't think that Brexit is going to have an impact on MiFID II. I think the FCA have already said that leading up to Brexit that the UK will be 100% compliant with EU regulations. I think post Brexit we'll have to wait and see. However, I do think that if UK financial services businesses want to be selling their services in Europe, they're probably going to have to remain in line with EU regulation, but I think we'll have to wait and see. PRESENTER: So Gill, let's now look at transaction reporting. So there's going to be so much more additional data that funds are going to have to deal with, I mean what's your advice in this area? GILLIAN BOSTON: I think again, I mean when you think about we're going from 28 data fields to up to 65 fields, in fact there's more actually hidden behind the scenes if you like, if you're using an arm. An arm will actually want additional fields as well. So it's 65 plus. So the amalgamation and consolidation of that data, that's not an easy thing to do for organisations, particularly where they're trying to take, well they have to take data out of operating systems that aren't designed for regulatory reporting. So again there's a lot of money already been spent in regulation, it's about finding that efficient and effective way of doing that, and that's where the likes of technology can really help. Because I think certainly under MiFID I there's still mistakes made with transaction reporting now. So to take that jump to MiFID II is a big ask. PRESENTER: Well, what sort of mistakes are we looking at? Because obviously as you said there were a lot of breaches with MiFID I, I mean give me an example of that and what are the grey areas with MiFID II, are there any? GILLIAN BOSTON: Well certainly if you think about MiFID II and there was an exercise the FCA did, albeit a couple of years ago, and they took one week's data, they looked at four or five data fields, and within those four data fields, four or five data fields within that week there was something like 650,000 mistakes. So if you extrapolate that, and then extrapolate that further to the new data fields that are required, that just shows you the size of the issue. I mean if you think about transaction reporting and MiFID II as a whole, the FCA want to see the market as a whole, and so yeah I don't think they're going to take too lightly to certainly over-reporting. That's something they've made clear that they don't want to happen, as well as under-reporting. So yeah, you really need to be on top of that. PRESENTER: So let's look at tech solutions then, what can they do? GILLIAN BOSTON: Well, I suppose, as I've already mentioned, you are typically trying to fulfil regulatory reporting obligations from operating systems. The data is all there, but how do you manage that data in an efficient and effective way so that you have the transparency of data, the good governance around that data and the auditability of that data as well. So that's where tech solutions can really help with respect to the data management. And it's not just from a regulatory reporting perspective, think about what you can do with that data from an MI perspective for helping make operational decisions. So it's about really being able to surface data in a different way that's perhaps difficult to do if it's manual processing or spreadsheets, or even if there is a database there already, which is a bit of a black box and you don't have that true transparency of data that you need. PRESENTER: So how can companies review existing data, and is it too late to actually put an in-house solution in place? GILLIAN BOSTON: For MiFID II, I would

absolutely say yes, given that it's, we're nearly into quarter four. I think, I touched on the senior managers regime, and I do, certainly last week Jonathan Davison, who is an executive director at FCA, he's talking about the senior manager regime as the accountability regime. And I think that leverage may actually make firms say hang on a sec, we really need to get our house in order here and have much more control and transparency over their data. So that coupled with additional regulation, CASS, MiFID II, etc., maybe this is the catalyst for actually firms recognising that they need to have better solutions in place in-house. PRESENTER: And almost to reiterate that point, how important is transparency in solutions? GILLIAN BOSTON: I mean again it's fundamental. It was actually interesting what Jon was saying with respect to GDPR. It's about having demonstrable audit evidence, demonstrable process. You have to prove and show what you're doing, and you can say this is what we're doing and this is why we're doing it. And then you can be challenged on it. But yeah it's fundamental. PRESENTER: And Anastasia, a lot said about transaction costs and charges. Talk me through what people need to be aware of. ANASTASIA GEORGIU: Yes, so there's some new data points that are coming. So asset managers will be providing additional data points. So around fees these will come into four buckets, and there'll be data on expected costs that will need to be used in the presale fee disclosures, and actual costs which advisers will need to use in the post-sale fee disclosure. So the fees fall into four buckets. You've got one-off charges, so things like initial fees, switching charges, exit fees. You've got your ongoing charge, you've got performance fees, and then the newer one is really the transactional fees, which asset managers are going to have to provide to the distributors. PRESENTER: So, Anastasia, I mean I read that nearly half advisers in the UK expect MiFID II to have a negative impact on the financial advice industry, and the majority believe it will lead to an increase in restricted advice. I mean what are your thoughts on this? ANASTASIA GEORGIU: So I think any time there's new regulation coming into play there's always concerns, and there's always quite a negative view on it because obviously it's more work, cost, time and effort, all of that. So I think actually it's not going to have a massively negative impact. And I think the reason for that is that I think there'll be more adoption of technology. So Gill was talking about it earlier, I think technology is going to really help to support the processes that need to be in place, help to deliver the new data that the advisers are going to need to have access to. And there'll probably also be maybe a shift towards more outsourcing of investment solutions, like model portfolios and managed solutions. In terms of do I think this is going to push more advisers to become restricted, I mean to some extent yes. But I think primarily because they could be both restricted and independent, I think we'll see even more segmentation within firms to offer different services to different client types. PRESENTER: So how will the advice process change? ANASTASIA GEORGIU: So, in terms of the advice process, there's additional product governance. So we've got new target market data that advisers are going to have to assess, so that the manufacturers are going to be providing target market data that describes who the product is aimed at. But also who it's not aimed at. So I think advisers are going to have to assess that information and make sure that their product line-up, their models are in line with the customers that they're delivering those solutions to. They're also going to need to be able to have a mechanism for communicating back to the manufacturer if for example they advise on a single product that is not in line with the target market. So that's new, and that's something they're going to have to take into consideration. In terms of the actual investment advice piece, they've got the additional need to assess the client's suitability on an annual basis. And I think there's obviously the issues around having to do additional work on the fee discloser. So they're going to have to provide their clients with a total cost of investing that includes not only the product fees that we talked about a few moments ago, but also any service fee. So that could be their advice cost, any platform charge, any discretionary fee that's being charged. So they'll have to provide the clients with that sort of total cost, and they'll have to show them what is the impact on their expected return. PRESENTER: And when it comes to risk profiling, what should be advisers be aware of? ANASTASIA

GEORGIU: Well I mean again I don't think it's a massive change, but MiFID is quite explicit in that when the adviser is assessing the suitability of their client, that they make sure that any tools that they're using are fit for purpose. So they're going to really have to have a look at their risk profiling tools or any tools they're using, and basically assess whether or not there's any gaps in terms of what the tool can do, and then basically mitigate against that. PRESENTER: So how would you suggest then that industry professionals really stay up to date with all the regulatory change? ANASTASIA GEORGIU: I mean there's quite a lot of information out there, so ESMA has really good Q&A which they can access. The FCA have put out the policy papers. And then there's industry bodies that also have documentation and details about what you need to do, and providers like ourselves also put out information, so there is a lot out there. PRESENTER: And Gillian, what would you say are in the works moving forwards, to summarise what should people be aware of? GILLIAN BOSTON: I think they should be aware that regulation is not going away. I do think, I know we were talking about Brexit, but I always think the FCA and certainly in the UK we're always seen to have the gold plated standard. So I don't think it's going to change significantly. I think that firms themselves are in a strong position if they think about it from a holistic approach. Because a lot of the time the data you're reporting for one regulation is actually needed for another regulation. And if firms are going to grow, organisations are going to grow, which of course they all want to do, it's really about having that holistic approach, and having the flexibility and adaptability to be able to change quickly if regulation itself, which it typically does, does change as well going forward. PRESENTER: So Anastasia, what would you say then are the biggest challenges facing the investment management space moving forwards? ANASTASIA GEORGIU: I mean I think for right now it's really the time to get to the implementation of MiFID and the work they have to do. PRESENTER: And Gill? GILLIAN BOSTON: Yes, I would agree with that. And I think it's perhaps looking to make sure the processes that have been put in place: are they sustainable, are they maintainable? We know a lot of money has been spent in the industry already in readiness for MiFID II, but actually has what's been put in place, does that need to change after go live as well? So yes, I think there's quite a challenge going forward. PRESENTER: And Anastasia, what would you say are the main takeaways for advisers from this Akademia session? ANASTASIA GEORGIU: So they really need to get started if they haven't already. Get started, start looking at the processes you have in place. Look at that around suitability, product governance, so make sure that any systems that you're using are fit for purpose. Make sure that you're going to have access to that new target market data, and think about how you're going to disclose your costs. And I think if they start with those streams they'll be in quite a good position. PRESENTER: Good, Anastasia, Gill, thank you. BOTH: Thank you. PRESENTER: In order to consider the viewing of this video as structured learning, you must complete the reflective statement to demonstrate what you've learned and its relevance to you. By the end of this session, you'll be able to understand and describe why good CASS governance and oversight matters; GDPR, what it is and who it affects; and MiFID II and how prepared firms are to address it. Please complete the reflective statement to validate your CPD.