TERES

INDIA ADR WEEK 2026 – 08 SEP 2026

SESSION 2

DATA PRIVACY IN CROSS-BORDER ARBITRATION: DPDPA, GDPR AND BEYOND

SPEAKERS:

MODERATOR: S.M. ALGAUS, PARTNER, CMS INDUSLAW

AMRITA SINHA, HEAD CORPORATE LEGAL GROUP COMPANIES, TATA STEEL

SANDEEP CHOWDHURY, GROUP GENERAL COUNSEL, SUZLON ENERGY

SHREYA SURI, PARTNER, CMS INDUSLAW

ANUSHKA MANSHARAMANI: We request everyone to please take your seats. We will begin with the next session in about 2 minutes. Thank you. We would now like to begin with our second session for the day hosted by CMS INDUSLAW. As arbitration becomes increasingly international and increasingly digital, the volume of information moving across borders has never been greater. Personal data, confidentiality of documents, evidence and sensitive commercial information are now integral to modern arbitral proceedings. This brings us to an increasingly important question - How do we protect that information while ensuring that arbitration remains efficient and effective? Our next session addresses this very issue. "Data Privacy and Cross-Border Arbitration DPDPA, GDPR and Beyond." This session will be moderated by Mr. Algaus. Joining him we have Ms. Amrita Sinha, Mr. Sandeep Chowdhury and Ms. Shreya Suri. I would now request everyone to please come on stage. Thank you.

S.M. ALGAUS: Good morning, everyone. Welcome to what I expect to be one of the most practically valuable sessions. My name is S. M. Algaus. I am a Partner - Disputes in CMS INDUSLAW, and I have the privilege of moderating today's discussion. We are gathered here at a genuinely important moment. The Digital Personal Data Protection Act is rolling out its substantive obligations in stages; the final and most consequential tranche of course coming by May 2027. That is not a distant deadline. Now, for anyone in this room who deals with personal data in the course of their work, that clock is ticking.

Now you might reasonably ask what is data protection law have to do with arbitration and cross-border arbitration at that? The answer, as our panel will demonstrate over the next hour, is far more than most practitioners anticipate. Here's the key insight. Every cross border arbitration processes some element of personal data. The moment a Request For Arbitration is filed, personal data could be in motion, Witness Statements, employee records, custodian correspondences, material produced on disclosure, transcripts and recordings of hearings, the case file maintained by the institution itself, all of it could have personal data. All of it attracts some element of compliance obligation depending on the regions and the regime applicable to it. And not one of those obligations disappears simply because the Parties have chosen arbitration as therefore.

Separately, there is another dimension that makes today's discussion particularly interesting. Data protection law can itself be the subject of arbitration. Data processing, agreements with an arbitration clause, a breach of that agreement, a contractual claim against, or rather between the Parties who are also subject to a statutory regulatory regime. That raises a fascinating question - Can a dispute arise under data protection legislation even be referred to arbitration at all? I have the privilege of introducing a panel that brings together three

1

perspectives that this topic really demands. The regulatory law specialist, which is Shreya, the in-house Counsel at a global corporation, Amrita, an in-house Counsel at the heart of a major industrial group, Sandeep.

Starting with Shreya Suri, Shreya is a Partner at CMS INDUSLAW in the Technology, Media and Communications Practice. She specialises in data protection, Fintech and data in digital intermediaries, and has advised extensively on DPDPA from its inception, including on data governance frameworks, consent architecture, breach response and the interface between Indian law and GDPR. If anyone in India can tell you exactly what the DPDPA means for a cross-border arbitration, it is Shreya.

Amrita Sinha. Amrita is the Head of Corporate Legal for Group Companies at Tata Steel. She has over 19 years of in-house experience, spanning complex cross border M&As, prominently the acquisition of Bhushan Steel through IBC route and corporate governance across India, Europe and beyond. Amrita knows what it means to manage data flows across multiple geographies, multiple subsidiaries and multiple regulators. That is exactly the practical lens we need today.

Mr. Sandeep Chowdhury. Sandeep is the Group Counsel for Suzlon Energy Limited. He is the recipient of the legal 500 GC Powerlist Award, BW World Top 100 GC and distinguished legal minds from legal ERA being many of the accolades that are attributed to him. He has managed large multi-jurisdictional legal operations across complex litigations, arbitrations, M&A and regulatory matters. Sandeep's value to today's session is that he has to make these complex decisions work in practice, with real timelines, real constraints, probably, and real consequences.

Together, this panel represents the full arc of answers to the data privacy problem in international arbitration from, is it even arbitrable through, to which law actually applies. That is the journey we will take today. Welcome everyone. Let us get started. Our discussion today moves through five connected themes which we hope to cover in the next 50 minutes. Whether data privacy disputes can even be arbitrated, which data protection regime governs cross border arbitral record, what practical risks are for in-house teams during a live arbitration, what happens to all the data once the award is rendered, and what can actually be done concretely at the level of first Procedural Order and beyond? We will leave roughly 5 to 10 minutes for questions at the end.

Now let us begin with a question that sits at the threshold of this entire topic and one that practitioners advising on data processing agreements should have a clear answer to before

they need one. So, Shreya, here's the scenario. A data fiduciary and its data processor have a Data Processing Agreement. It contains an arbitration clause and there is a significant breach; personal data is exposed. Data fiduciary wants to arbitrate. The processor says this matter belongs before the Data Protection Board of India under, say, the DPDPA once it is formed and not the Tribunal. Who is right? And the second part to it is, does Section 39 of the DPDPA which bars civil courts from entertaining suits in respect of the matters of which the board is to be the final determinant, change that answer?

SHREYA SURI: Thanks, Algaus. Interesting question. I, at the outset, just want to clarify a couple of things. The Data Protection Act in India does not explicitly obligate or bind data processors statutorily in any manner. Most of their obligations, or rather majority of their obligations will be driven by the contractual terms they have entered into with data fiduciaries. At the end of the day, any dispute arising from that contract will be treated as a contractual dispute. In... So, in this scenario that you've set out, if there is a breach of obligations that the data processor has carried out, or rather there's an omission in its obligations that it was supposed to carry out, the data fiduciary will have a right, you know, depending on how the contract is structured. If there's an arbitration clause, they will be bound by that arbitration, *inter se* between the Parties. That's a private contractual issue. But when it comes to any individual trying to exercise its rights under the law, that will fall before the Data Protection Board directly. They don't necessarily need to get into the contractual contours of what the data fiduciary and data processor have agreed to. If there is a breach, that will be directly subject to data fiduciary not resolving that breach; that will be directly reported to the board. The board can then call upon and will then call upon only the data fiduciary to answer and respond in relation to any such complaint.

Depending on how you've contractually agreed in respect of the treatment of third-party claims, the data fiduciary may call upon the data processor to step in and assume the defence and control how the proceedings take place. Again, all of that is agreed on a contractual basis as per standard contractual terms, you would have those indemnity clauses. But an *inter se* dispute will likely not be taken to... I mean, the right, the correct authority to adjudicate would be either a civil court or an arbitration authority, depending on how the contract is structured.

S.M. ALGAUS: Fair enough. So, from what you have said, headline is that the contractual dispute between a fiduciary and its processor is ordinarily arbitrable under the Indian law and it runs between those two contracting Parties. The board's jurisdiction is a parallel track confined to data principle's complaint, and that's a statutory complaint, and they run simultaneously without any conflict. Okay, fair enough. Thank you, thank you, Shreya for that.

Now, there is another follow up question I would of course ask you, because before we lay the groundwork for the rest of the risk management and the procedural bit, that of course, Amrita and Sandeep can contribute to. Let me give you another scenario. Now this more or less on a cross-border basis. I suspect that it is not a hypothetical one considering the topic. Say an Indian company, and the arbitral seat is in London, the counterparty is based in EU. The document review vendor is based in US, the Arbitrator is sitting in Singapore. There are five participants, and potentially, there are four distinct data protection regimes and there is only one arbitral record. The natural instinct would be to ask which law would govern the flow of data during these proceedings? So, what exactly would be the parameter to determine where and in what manner which regime applies?

SHREYA SURI: So, there are three to four factors to consider for any contract of this nature or any dispute of this nature. First and foremost, when the Parties are entering into this contract, they need to understand which is the jurisdiction where personal data, or the individuals whose personal data will be used, which jurisdiction do they ordinarily belong to? Any laws associated with that jurisdiction which cover, you know, the personal data of those individuals, will need to be understood and complied with by both the Parties involved. So, let's say the data belongs to EU residents, your residents of EU member nations, the EU GDPR would apply. And if the Party, as you said is an Indian Party, maybe that's the processor, I'm not sure in this hypothetical example which one is which, but assuming that the processor sits in India and the data belongs to EU members which is being passed on under contract, the Indian Party would also be bound to comply with whatever compliance requirements exist for data processors under the EU GDPR.

Now as far as the Indian Party is concerned, because I'm assuming it operates within India and its primary business activities are in India, all its obligations will be driven by contractual provisions that would be enforced on the Indian Party, and the legal statutory provisions of EU GDPR are mandated to be contracted as standard contractual clauses. So, those statutory provisions and terms would all already be built into the contract, which would then entail that any breach, again, goes back to... any breach of the contract would also fall within the realms of, (a), a contractual dispute, (b), it may also have a direct implication or liability under EU GDPR laws if the processor is directly subject to such laws. If they are only subject to such laws through the data fiduciary and the contract that they have executed, then only the contract will govern. But if the data processor is also independently subject to EU GDPR laws, they may have direct statutory liability under those laws as well.

If there is an arbitration, the governing law of the contract will have to be determined accordingly, and that will guide which law takes precedence. In this example, it is very likely that the governing law may be... I mean, maybe the laws of Germany or France or whichever jurisdiction this may relate to. And even if an arbitration is taking place elsewhere, that law has to be... I mean, the jurisdiction associated with any kind of legislation or governing principles that flow from that law, will have to be incorporated into the procedural arbitration requirements; that would either be of Singapore or London, I forgot which one you indicated. And that's the way, it will play out. So, again, there would be... if it's a private dispute between a data fiduciary and a data processor, the same principle will apply; it will be treated as any kind of contractual dispute, but there can be a parallel statutory liability depending on whether or not a particular law applies to you.

Now let's say the role is reversed and the Indian Party is dealing with data of Indian individuals and EU individuals. So, there could be statutory liability in both situations or coming from both laws. That will have to be factored in independent of the contractual positions of both Parties.

S.M. ALGAUS: Okay. Thanks, Shreya. So, just to synthesise this from what I understand, what you're saying is that the data protection regimes do not follow or they are completely agnostic about the seat of the arbitration or the governing law of the contract or the nationality of the arbitrators, either ways. What actually they follow is the data subject or the data principle. And the question is not which law would govern this arbitration, more or less which law would attach to the individuals who are being processed as part of that particular dispute. Would the question of the regimes applicability come in?

SHREYA SURI: Yes. And any contractual dispute would be treated separately.

S.M. ALGAUS: Separately. Correct. Fair enough. Fair enough. Thank you thank you, Shreya for that. Now let's move from the regulatory architecture to what it actually means to be the person responsible for it inside, say a company that is in arbitration. General Counsels and in-house teams are increasingly expected to treat data handling in dispute resolution as a live compliance item and not an afterthought. In this regard, Amrita, from an in-house Counsel perspective, what are the key data protection risks that arise in a cross-border arbitration and how do you manage those risks without compromising the company's ability to prosecute or defend the arbitration effectively?

AMRITA SINHA: Thank you. Thank you for that question. Am I audible? Yeah. So, you know, I'm going to keep this very practical. You know, there are practitioners here who know

the law you know better than I do, but I'm going to keep it to an in-house practical perspective as to what I, you know, foresee as the risks in a cross-border arbitration exercise. So, you know, there's this fundamental shift, and I want to start this with, you know, background of the fact that, you know, after ***Puttaswamy vs. Union of India***, the there's been a fundamental shift in the way that we are looking at data is now property it is a property that is, you know, that belongs to a particular person and individual as defined under the Act. And therefore, you know... we can't just you know, we can't we can't just collect it, we can't process it in the manner that we like. So it is somebody's property, it has to be... And the Constitution has said that it is a fundamental right of a citizen under Article 21, that that data of that individual has to be protected. So, for General Counsels and in-house teams, I'm sure Sandeep will agree that I think it is a greater duty upon, you know, companies now who are collecting data who are processing data to look at this whole aspect of data protection, not just as, you know, a compliance, a regulatory risk or, you know, maybe a risk management internally, but more of a fundamental duty to protect, you know, the right of a citizen, of an individual.

So, with that in mind, I think to answer what you asked, Algaus, is from a cross-border data protection perspective, what are the risks? You know, cross border data, cross border arbitration very quickly becomes a, you know, a data sharing exercise between jurisdictions. Typically in a multinational company in any case, there's a lot of data which is moving around different jurisdictions at all points in time. So, it is a harrowing task. Given an arbitration of course, at different points in time during the proceedings, there is a lot of data that you would have to present to substantiate your matter, and you cannot of course take a position that there is a restriction or there is a law. Of course, there'll be a restriction but you'll have to work around it.

So, you know, with that in mind, it becomes important. I think there are three things from a practical perspective that I would focus on. Number one is data minimisation. Usually, arbitration teams, when they come back to you, Counsels, External Counsels, there'll be there'll be several Parties that you'll be dealing with and sharing data with. There'll be there'll be the Tribunal members, there'll be you know, these e-discovery platforms, technology platforms that will be sharing data with. And usually arbitrations and External Counsels will come up with a requests of a huge humongous amount of data from you. Maybe that that's the point in time where you should think that where is the minimisation that is required, what exactly is required. You can't just pick up an employee database and just put it together and send it to the External Counsel; that just exposes you to risks. So, data minimization is one.

The second point that you know, I would keep in mind of course is, you know, privacy versus confidentiality. This is an important fact from a data protection perspective to understand, is that, just because the arbitration proceeding is a confidential proceeding, it doesn't mean that you can share all the data, and of course, specifically personal sensitive data. So, you know, though it is a confidential... though arbitration is a confidential proceeding, we should keep in mind that when you're transferring data between jurisdictions in a cross-border arbitration, you keep in mind where the employees are based, whose data are you sharing. If you're sharing consumer data, where are they based, which are the laws that are applicable. That's number two.

Number three, I think you should learn... and this from the very beginning when the process begins, you can't start this whole governance process when the arbitration is already midway. I think all of this you should think and start at the beginning of the arbitration process, and that is data governance. Data governance is basically how will you transfer the data, what are the access controls, what are the cyber security measures that your organization should take before putting in... putting in the data together, and how will it be shared with all these different external Parties, with whom data must be shared? So, I think these things are important from an in-house perspective to consider before even an arbitration begins.

When a proceeding begins, you as a Counsel are you know... you hold... you're wearing two hats. One where you're looking at the merit of the matter and you have to substantiate the arbitration; that is one part, but it is also very important to see how the data flows from a data protection perspective. And of course, the in-house Counsel is the custodian and sitting with, you know, that piece of it. So I think those things will certainly be relevant to the risks... the risks I see from a practical perspective and how you can, you know, maybe mitigate them. Thank you.

S.M. ALGAUS: Fair enough. Thank you, Amrita. I think what you've touched upon is something that is quite underappreciated - the gap between the data protection compliance framework a company has built for its ordinary commercial operations and what it actually needs to do when it finds itself in an arbitrary proceeding. Now, I think naturally this... Yes.

SANDEEP CHOWDHURY: I just want to add something that Amrita has stated. I think I totally echo on the fact that, you know, in the current situation how managing data within the organization has gained importance, right? So, I head the entire enterprise Risk Management for my organization. So, you have the business risk, you have the geopolitical, the legal or the compliance risk and all. And I have seen over a period of time, say for the last one, one and a

half years, you know, managing this data risk is gaining importance day-by-day, right? We also have operations in, other than India in 19 other geographies; there's an inflow and outflow of data that happens and what's our control, what are the do's, what are the don'ts and all. There is a good amount of time which my team together with the IT team and all spent with the concerned stakeholders in terms of rightful management of the data. So that there's a seamless operation from the company standpoint, and also you don't want to be a bad boy at the end of the day, right?

S.M. ALGAUS: Right. Thank you. Thank you, Sandeep. Actually, that is quite valuable. I just actually was foraying to asking you the next question, if you just give me a minute. So, Sandeep, now there is the ICCA-IBA roadmap to data protection in international arbitration, and it is quite a robust and comprehensive single treatment of the subject. Now it talks about the First Procedural Order, the full data protection protocols, and it has precedents on the privacy notices for institutions Arbitrators, Counsels. Now, it's an extraordinary document, and in practice, the drafting of the First Procedural Order and the data protection directions that are supposed to be implemented in accordance with such established principles, frequently revolve around certain very fixed boilerplate clauses. Now Sandeep, from the perspective of a GC who receives reviews and is bound by a Procedural Order, the First Procedural Order and its directions in practice, what are the data protection clauses that actually you do find useful? What is the minimum or non-negotiable content that a First Procedural Order must contain to genuinely protect your organisation? If I was to just in a way rephrase it, what practical measures do you think that Procedural Order directions or these retention schedules and redaction protocols and diligence on hosting, can Parties, Counsels, Tribunals and institutions actually adopt?

SANDEEP CHOWDHURY: Thanks, Algaus. I think first of all, thank you for a nice introduction of the panel. Secondly, I think before I say anything, it's my personal view; nothing to do with my organisation *per se*. Procedural Order, the First Procedural Order, in any arbitration proceedings, I think it plays a very important role, right? It not only defines the timeline or the way the arbitration needs to be conducted. These days what we've also seen is that it is also touching upon the confidentiality part, it is touching upon data protection, it's touching upon the cyber security and all, right? It also lays down how you are going to deal with the confidential informations, whether it's ordinarily confidential or highly confidential or your personal information and all. And who would have the access of those information. So, from that standpoint, I think, it plays a very important role at the very first threshold.

Secondly, I think one of my panellists also touched upon a point on, we need to be judicious in terms of, you know, sharing the information, because in any arbitral proceeding, I think we share a lot of information. There is no sort of, discipline in terms of what information you're sharing. So, you know, basis that, you have to share information which are proportionate to that particular proceeding or you have to be very pinpointed when you're sharing the information. Now there can be situation that the Arbitral Tribunal may also ask from you about the redaction logs and all in terms of the personal information that you've redacted. So, that is also... that should form a part of the Procedural Order- 1.

The third important thing what I feel and which we often miss, is the data retention and the deletion or destruction mechanism, right? So, we collect a lot of data. Once the award is passed and all I think the Parties forgets about what is the sort of... where does the data rests and all and you know, what's the destruction mechanism. So, these days we are also seeing the Procedural Order taking care of the retention and the deletion of the data, what data you can retain up to what time, what's the deletion mechanism, when you can delete? Because there are certain legal or the regulatory peripheries that you would have to bear at the back of your mind. So, that also plays a very important role.

Then in terms of cross-border arbitration, I think, you know, both the Parties and the Tribunal, they should have... at least they should have done the basic due diligence in terms of the technicalities and the hosting platforms of the data, where it is hosted, who would have the access and then whether it's encrypted or not? So, things like this. So, again we are seeing this on I mean very recently I've just concluded an arbitration in which was having the seat in South Africa, but the law was SIAC. And that was an institutional arbitration. So, we've seen this followed out there.

Last but not the least, these are not the obligations which should rest on the Parties *per se* correct you have the Counsels, you have the e-discovery partners, you have the translators, the transcripts and all; they should also abide by the confidentiality of the information that's been shared. So, in a nutshell, if I may answer your question, I think these days, the way the arbitration is done, I think we are more moving to a data retention and a data, if I may call it, data management life cycle, which would include right from collection of the data to deletion, right?

S.M. ALGAUS: Right.

SANDEEP CHOWDHURY: And I think if this is followed properly, then we can see a move in the confidentiality clause in the Arbitration Agreement. I mean, right now it's just mere a

clause, but if all these things are properly followed, then it can also act as a good risk governance mechanism. So, this is very important, because you know, in today's scenario, we are all thinking of managing our risk and all, and data being very important or you know, it takes a top seat if... And I'm sure there would be other things. But to me these are the top four or five things. If we can follow this, then we would be able to shift the needle from just having a clause in the agreement, to a proper data management mechanism.

S.M. ALGAUS: Fair enough. Fair enough. That's quite a detailed and very, very accurate insight into this whole situation. Now this brings me to, again, Amrita, because I think this feeds into the next question that I intended to ask you. Now in a cross-border arbitration, an Indian company may share personal data with foreign law firms, experts, arbitral institutions and e-discovery providers, just like how Sandeep had just contemplated in his response. Now, under India's data protection framework, to what extent can a company rely on these external advisors? And what should an in-house Counsel do to ensure that data remains adequately protected?

AMRITA SINHA: Thank you for the question. I think as soon as you say that you are, you know, interacting with all of these third-Parties for the purpose of course, cross-border arbitration in this context, you then quickly... you know, what you're doing is you're delegating the handling of the data, you know, to a third-Party. Under the DPDPA, if you look at the Indian context, I as a data fiduciary who's collecting the data, I am not relieved of my obligations as soon as I give my data to a third-Party, you know. They could be Tribunals, they could be Witnesses, they could be these e-discovery and technology platforms that we are dealing with when we are managing this whole cross-border arbitration process. So, given that I am not relieved of my obligations, and in fact, DPDPA casts upon the data processor a higher responsibility with respect to data breaches, even if done by a processor. So, you know, the obligation lies with the fiduciary. It's unfortunate but that's how the law is. So, I think when you're sharing, of course, you know, information with your external Counsels, with third-Parties, I think two things again, from an in-house perspective that I would be careful about is, number one, diligence of your third-Parties, your vendors that you're dealing with. You know, there may be technology platforms that may be, you know, less expensive, so to say, there may be lawyers who may be more efficient, maybe smaller outfits or whatever, you know, that is a more general comment. But yeah, there may be smaller outfits with a more cost efficient from an arbitration perspective. But when you're looking at arbitration, it's not just the matter; it's also, like we're talking about the whole data protection angle that we're looking at. And therefore, it's important to make sure that you do a due diligence of all the third-Parties

that are involved in this process, whether they have the wherewithal to protect your data that you will be sharing with them. So, that's one angle I think that's something that I personally think that we should look at very keenly. Who are these e-discovery, smaller technology platforms that we may be using during this process?

The second thing is of course contractual obligations. You know, given that you have the ultimate responsibility, you will definitely want to get into, you know, very tight contracts with each of these people that you are sharing data with, and of course, cover matters and confidentiality, matters on access control, matters on whether they will be subcontracting, whether they will be sub processors and how they will manage the data. So, those are two kind of, I think, things are kind of highlight that I would certainly take care of while sharing data with third-Parties.

S.M. ALGAUS: Thank you. Thank you, Amrita. Now Sandeep, again, because this is kind of an interconnected situation. Now in a major construction arbitration, now multiple Parties are involved; there may be a principal employer, subcontractor, specialist, consultants, and they are pooling records as a matter of shared e-discovery and a case management platform. Everyone has access and everyone is contributing documents. Now under data protection law, at the point those Parties jointly decide what the platform holds and how it is used, something important, I think, changes. So, Sandeep, when do these Parties cross the line from an independent controller processing their own data into say, joint controllers sharing one? And who bears the liability for the platform if it is breached?

SANDEEP CHOWDHURY: Sure. I think before that let's go take ourselves a little bit backward in terms of understanding the concept of the controller per se, because it is there in the GDPR, but under DPDPA there is no concept of controller; it's the data fiduciary and the processor. So, basically, a controller is nothing but someone who sort of, has the... who decides and who has the means or the purpose of doing the data processing, correct? And under if I go into the DPDPA thing, then it is the data fiduciary who is, at the end of the day, responsible for non-compliance of the data processing and all, whether it's been done by itself or on its behalf by the data processor. And it is also the data fiduciary who lays down the proper checks and balances and have the security measures in place, and would also sort of, inform if there is a data breach, right? Now coming to your... And then we go into a joint controller, which is almost similar to, you know, an individual controller. It's just that two or more organization, when they decide the purpose and the means of processing the data, they fall within the definition of "joint controller" and if I'm not wrong, I think it's under Article 26 of GDPR or something like that.

TERES

What is also important is, between these two organizations, there would be an internal arrangement, right? There would be an agreement in terms of what data, who would process and who would have control on that. Now if there is a breach, as you've sort of... you know, I think that's the last part of your question, if there's a beach in terms of... by the joint controllers on the data part, then the liability... Again, they can be jointly or severally liable, correct? That's what the Act says. But at the end of the day, the liability is also governed by what is the internal arrangement that they are having amongst them. So, it's not a plain and simple thing that, by being a joint controller the liability gets decided 50-50; that's not the situation. Now the entire thing on the indemnity or the contribution part depends upon what is the internal arrangement that you are having amongst yourself. So, that's very important and that's how the regulators also decide. Even if you write, and most of the time we've seen in the agreement that, you know, we are we are writing that we have hovering more on the individual controller, we care less about the joint controller part. Even if we write about joint controller, we don't define the, you know, the internal relationship between the joint controller - who's going to decide what, at what point of time, and in terms of breach who would be liable, correct?

So, to me, I think, if I look into the concept of an individual controller *vis a vis* a joint controller, when there is a breach, I think the individual controller is much better off because he knows what he has done because of which the breach has occurred, and what's the rectification mechanism and all, that's also sort of known to him. I think it becomes a little bit murkier when it comes to joint controller, again, because of the fact that you can be jointly and severally liable for fault you never know which been done by you or done by the other side or the other Party and all. But the fact of the matter remains that, again, the internal arrangement between the Parties needs to be very strong. So, if the internal agreement that's been pinned down does not capture the scope of each of the Party with regard to data processing, then I think the life of the joint controllers become even more murky.

So to answer your question in a nutshell, that internal arrangement; very important. Joint controller, again, they can be liable either severally or jointly. And it does not typically it's not a 50-50 mechanism. And so, if there is a breach at any given point of time, say if there's a breach at whatever hours of the day, if by looking into the arrangement if I could figure out the breach has occurred because of whose fault, it was in whose scope and who would be penalized, correct? If I have these three answers in place, then I think I have penned down the internal arrangement properly. If not, then it's a... again, it's a problematic situation. So, I think that's the answer that I have for your question that you've raised.

S.M. ALGAUS: Thank you thank you Sandeep now this actually brings me to... Shreya, you want to say something?

SHREYA SURI: Yeah, yeah. I was just going to talk a little bit about, you know, we've been using the word 'breach' a lot, and I do want to point out that it is defined differently in the GDPR and the DPDP Act. And the way you define it in the agreement should mirror the kind of responsibilities you want the other Party to undertake. So it's very, very critical. In India it is any kind of... statutory definition is any kind of unauthorized access to personal data, which means even a mis-delivery of an email within your organization could potentially qualify as a breach. So, there are very far reaching consequences for the way we even define terms, the way we define, as Sandeep also pointed out 'controller' versus a 'fiduciary'. In India there's no concept of a... there's no defined concept of a joint data fiduciary. But if you closely see the definition of 'data fiduciary', it talks about the possibility of another data fiduciary being a part of that definition. So, very important to just be clear, as much as possible in contractual terms, in terms of how liability and risk needs to be allocated.

S.M. ALGAUS: Yeah. Yeah yes please, Amrita.

AMRITA SINHA: This is a... I'm sure corporates everywhere, I'm sure this is a discussion that will go on at all places, that this... the fine, the penalty amount that the law and the schedule to the law talks about for data fiduciaries for a breach. And not just by the data fiduciary but also by the data processor, which the data fiduciary is liable to pay, that amount is currently up to 250 million in the legislation. We know that this is not played out, you know. We've seen CCI... and CCI, of course Competition Act also does talk about, you know, turnover related, you know, penalties that are... fines that are payable. But we've seen CCI and how it's panned out. But this 250 million, the number, you know, that, and of course companies have dealings with various kinds of third-Parties. So, the processor may be large and small. There can be large companies and there could be very small companies who say are managing a guest house for you or managing a hospital for you. So, for them, that number is very startling. So, you always want to keep... like, you know, Sandeep was explaining, you know, back-to-back agreements, you want to keep your liability. Given that you are exposed to that kind of fines, you want to keep it open for third-Parties. I'm sorry for digressing from a cross-border arbitration perspective to generally and otherwise. But yeah, I'm very keen to see that how the law actually pans out when it comes to the fines part of it for data fiduciaries.

SHREYA SURI: Yeah, I actually have a little bit of insight on that since you brought it up, and I think very relevant for the audience here as well. First and foremost, a real kicker is that

if there's a personal data breach, yes. You know, if you did not take steps to prevent that breach, the penalty can go up to 250 million. But it is very likely that there could have been other violations under the Act as well, which have their own penalties attached to it. So, the penalty could be cumulative and even go beyond the 250 crore threshold prescribed. Now interestingly, with respect to the 250 crore penalty amount, the language says that "if security safeguards were not in place or reasonable measures were not in place". So, there will be mitigating factors and any... I mean, any complaint dealt with by the Data Protection Board will look into those mitigating factors before determining a penalty. Because let's be real, data breaches are going to evolve, they're going to happen, many best practices will be adopted by organizations which will become the norm, they will become market practice. But despite best efforts, sometimes breaches can happen. So then, it will be how you position your mitigating factors. Like you were saying earlier, Amrita, did you do a vendor diligence? Did you... as Sandeep was also talking about, did you have protective clauses in your contracts? Did you ensure that you were sharing data responsibly, you were minimizing the data, you were sharing, was the purpose limited? So, all these will be factors to mitigate any kind of penalty that could potentially be levied under the Act, and that's why very important to have data governance, good data governance in place.

S.M. ALGAUS: That's right.

SANDEEP CHOWDHURY: So, I think one point I do agree with you and with you also Shreya, is that there's a back and forth which is happening with regard to the amount which is mentioned in the fine. It's not only 250 crores but I think if you don't report it's some 200 crores or something like that, right? The regulators are also collecting... it's a WIP to me at this point of time, the regulators are also collecting certain industry-related papers. And what I see, the way they are moving towards, is putting a cap on the fine and linking it either to your top line or bottom line, correct? To me, that's a more rational way of doing things and pragmatic way, rather than just, you know, one-size-fits-all. So, I see there's a lot of movement towards that direction. I mean, sooner or later, we would see some sort of a notification penning it down. But unless and until that happens, at this point of time, we'll have to leave with that 250 and 200 figure.

AMRITA SINHA: But the trouble is also this Sandeep is that it's not linked to... it may be you know, you're right, the percentage might just be linked to the data fiduciary's numbers rather than the processor's numbers. The processor maybe an entity which is a very you know, smaller outfit like I was explaining, but the linkage that the law, it seems will draw is with the

turnover of the processor. I mean, that's something... I don't know if there's any discussions going on in some corner.

SANDEEP CHOWDHURY: See, if that happens, then the amount of the or the quantum of file will reduce a lot, right? Because the processor, as you rightly stated, would be a smaller fish compared to a data fiduciary. I think one thing we'll also have to agree at the back of our mind, is that, this entire thing is very much in an evolving stage, correct? As it attained the finality, I don't think it has attained the finality, I mean, definitely they have come out with the Act and they've penned it down.

AMRITA SINHA: Some parts.

SANDEEP CHOWDHURY: But some parts of the rules also, but I think it's... you know, unless and until there are certain violations and how the courts are also looking into those violations and all, I think that could also lay down at least some sort of an incident to follow.

AMRITA SINHA: Yeah, as and when the jurisprudence, we'd get to know how.

S.M. ALGAUS: Fair enough. Actually, this is what I was actually building towards to ask Shreya about. Now basically the friction point could be the fact that there are differences in the way GDPR assigns liability and how DPDPA does. Now in view of that Shreya, the GDPR makes the processor somewhat liable to the data subject or the data principle as in India, but the DPDPA channels all liability to a fiduciary and leaves the processors exposure somewhat entirely contractual. In a cross-border arbitration where there's this multinational subject to both regimes and there's a possibility of application depending on whose data actually is being shared, how does that divergence change the way? Say for example, if you were to draft a Data Processing Agreement with an e-discovery vendor, and does the litigation strategy ever factor in to that entire approach to drafting a Data Processing Agreement in this situation?

SHREYA SURI: Okay. So, just two things I'll call out before I dive a little bit into the answer. Under the Indian DPDPA Act, there is an exemption. Similar exemption, not in so many words, is also brought under GDPR. The exemption is that certain provisions of the Act do not apply to a data fiduciary if they are enforcing their rights under a legal contract. So, ordinarily, an arbitration will fall within that bracket. Any data you share for the purposes of any dispute or any litigation with third-Parties, including e-discovery vendors, to a large extent, will not need to comply with the laundry list of compliances set out under both legislations. But at the same time, core principles which define data privacy as a concept, would still need to be followed, simply from the perspective of ensuring that reasonable security safeguards and

measures are taken before any data is shared. Because while other provisions of the Act are exempt, this still continues to apply. And that is the thought process with which any kind of contractual terms with a data processor, for e-discovery or otherwise, would need to be built in. So, same principles involving minimisation purpose limitation, try sharing masked information as much as possible, don't do data dumps. Ensuring that the e-discovery vendor has a baseline... you know, baseline measures for security infrastructure in place which meet the compliance requirements of the relevant law that is applicable to the personal data. Be it GDPR, be it India, ISO series is a good measure of the standards. GDPR is highly prescriptive. In India, they have left it open ended; so, you know you may need to do a little above and beyond as far as India is concerned.

But when sharing this information, when negotiating these clauses, be very mindful that the processor is only going to give up uncapped indemnification to the extent it relates to obligations that apply to it directly, which relate mostly in relation to security safeguards, at least under the Indian Act. Under GDPR, they are a little more extensive. And effectively, when negotiating these clauses, depending on which side of the table you're sitting on, you need to be mindful of the worst case scenario, you need to be mindful of how the contract has been drafted. But at the same time, you do have the comfort of those exemptions that are talked about, such that it is not wrong for you to share that information, it's just the degree as to what information you're sharing, how you're sharing that information, how that information is stored, is going to be relevant. So, those are the three things to fight for in any such contract with third-Parties.

S.M. ALGAUS: Thank you. Thank you, Shreya. That's quite insightful. I see the clock is nearing almost five minutes here. We do have lots of questions to go around; the topic is quite vast. But I think in the interest of time I think I'll open the floor for questions, considering that if anybody would want to ask any questions to the panel on the discussions that we had till now. Yes. Can someone please hand over a mic to her?

AUDIENCE 1: Hello. So, actually I think as per the DPDPA, if a data principal tomorrow raises a grievance with, say the grievance officer or the DPO but like the Data Protection Board has the authority to suggest that it should go for a mediation or arbitration, in that case... So, like let let's take an example. If there was a breach or if there was an issue with the consent that the data principal is not able to resolve like unable to recall that when the consent was given so in that case they reach out to the DPBI Board. So do you think in that case the DPBI Board can suggest the mediation like the arbitration option for that like that? Because that is the that is there in the Section 31 that only the Board can suggest that route?

S.M. ALGAUS: Sorry, I mean are you asking that when a Witness is given a statement and that statement is incorrect, you're saying he shared some information?

AUDIENCE 1: Like so, if the data principal had given a consent but they are unable to recall about that, and they raised a complaint but they find it unresolved maybe from the DPO or maybe from the grievance officer and they reach out to the DPBI Board.

S.M. ALGAUS: Right.

AUDIENCE 1: So in that case, the DPBI Board can suggest the arbitration method there like maybe some settlement there or like for the data principal point of view?

S.M. ALGAUS: No, I think if there is an actual region, of course I'll let Shreya address this as well, but if there is no apparent breach per se. There is no question of the principal assailing it before the board, but the Board will have to do the preliminary inquiry on this. Whether that is part of the contractual arrangement or not, I think, so far as the principal and fiduciary are concerned, their obligations are quite clear, and that is something within the domain of the Board. What actually falls probably out is when there is a contractual dispute, say between a processor and a fiduciary, in which case then that will be a subject matter of arbitration. Where the Board does have a mechanism for mediation, yes, arbitration according to me, is not exactly barred but it's not statutorily implemented. So, I don't see the Board making a reference to an arbitration for a grievance of this nature.

AUDIENCE 1: Okay, okay thank you.

S.M. ALGAUS: No worries. Yeah, otherwise any... I think there was another question over there in the middle. Can someone please pass the mic?

AUDIENCE 2: My question is to Mr. Sandeep Chowdhury. You highlighted how, you know data concerns issues are addressed in arbitration proceedings by, you know, laying it down in the First Procedural Order. I wanted to understand how are these concerns addressed when the arbitral award reaches at the stage of challenge before a court?

SANDEEP CHOWDHURY: So, again, it's very simple. If this concerns are penned down in the award, right? So, it is up to the Parties whether you agree to it or you don't agree to it and also you'll also there has to be a mechanism of this concern getting linked to the commercials, which is for you and against you typically if the commercials are against you. And when I say commercials is the monetary value in the award. If that is against you and the genesis of that is, you know, this confidential information or the entire thing on data protection and all, if

that's the genesis of reaching to that conclusion, then you will challenge the award under Section 34 and you would also take this as one of the pointers in 34. But what is the possibility of your success in 34, because now 34 the... even for challenging the award, it's become very narrow, correct. Honestly, I have never come into or I have never seen a situation where it's been challenged because of this grounds and then what's the outcome of the, you know, 34 court. But I would be interested in seeing that because you know, I... these days see, there's a lot of hue and cry about this during the course of arbitration proceeding but somewhere it loses its entire genesis when an award comes up. We only focus on challenging the merits of the award or numbers, whatever you call it, but I think this, if we look into a totality of the aspect, I think the genesis is something that also needs to be challenged. Again, as I told you, I have never come across any proposition of that such but I would be more interested in looking into as to what happens and what's the decision or direction taken by the court in these cases.

S.M. ALGAUS: Are there any other questions? Yeah, we're almost at time. We'll just take this quickly so that we can wrap up. There, right at the end.

SHIVANGI: Good morning everyone, I'm Shivangi. I work at Presolv360 which is an online dispute resolution platform. So, my question is anyone from the panel. For an Indian ODR platform, administrating a cross-border dispute which has Parties or Arbitrator, Counsels and cloud infrastructure all in... assuming all in different jurisdictions, who ultimately should take the responsibility for mapping and validating cross border data that is flowing in for process, assuming that the Institute has the role of a data processor?

S.M. ALGAUS: Shreya, do you want to take this?

SHREYA SURI: I can attempt this. I just want to make sure I've understood the question properly. You're saying in an online dispute resolution process, the authority which is facilitating the proceedings for the dispute is ordinarily getting control of a lot of information flowing in from different jurisdictions.

SHIVANGI: Yes.

SHREYA SURI: So, you're saying who needs to undertake the onus and responsibility for maintaining that data, is that ...?

SHIVANGI: Right. And assuming that the role of the institute is classified as data processor.

SHREYA SURI: Right. So, in this situation the Party which is sharing the information sharing... and here we are talking only personal data, right? Of course, confidentiality aside there is any kind of personal data which is being shared, the Party sharing it will be responsible for how it is treated. So, and any sharing needs to be done on the basis of a valid and binding contract. This is without prejudice to that exemption that I talked about earlier. So, ideally, the relevant Party will need to enforce and bind..., will need to bind the dispute resolution authority contractually for any kind of data that is shared and processed by them. So, storage, maintenance, maintaining the security of that information will need to be done by the processor in this scenario because that is an outsourced responsibility that the fiduciary or the relevant Party has imposed on that processor. And if that processor is engaging third-Parties or sub-processors, they would need to be bound by the same for flow down contractual provisions.

SHIVANGI: All right. Thank you.

S.M. ALGAUS: So, I think we are almost slightly above time. We'll close the session now. And I would want to extend my very sincere thanks to the panel, Shreya, Amrita and Sandeep. The depth and the practicality of this discussion reflects the best of what this panel has been able to achieve. And I thank MCIA for hosting this and for placing this topic on the agenda where it belongs. Thank you so much. That'll be all.

AMRITA SINHA: Thank you, wonderful session. Thank you.

ANUSHKA MANSHARAMANI: Thank you to the entire panel for an extremely insightful discussion. I would now like to request all the panellists to step down for a picture. Kindly note that the next session will begin at 12:00. Thank you.