Kluwer Arbitration Blog

Redefining Resolution in Data Disputes: Why Arbitration Holds the Key

Julien Chaisse (City University of Hong Kong) and Ishika Garg (Asia-Pacific FDI Network) · Monday, December 11th, 2023

In our data-centric economy, disputes related to the safeguarding, access and use of data are on the rise. That Microsoft has 'stashed' almost half a billion dollars in anticipation of a potential regulatory fine for allegations of dodgy data processing practices at its unit, LinkedIn, indicates that with big data comes bigger disputes. These disputes implicate personal data protection and privacy rights, which must be addressed with a nuanced understanding of both privacy laws and their intersection with dispute resolution. This post highlights the potential for arbitration to handle data privacy disputes, a realm traditionally reserved for public courts. Leveraging arbitration's strengths can ensure smooth integration of data privacy protection in our interconnected world, balancing individual rights with the ever-growing demand for data.

Contextualising Data Privacy

Data Protection Laws and Rights

Modern data privacy laws generally focus on safeguarding 'data subjects', the individuals whose personal information is being processed. To that end, they employ two central mechanisms: a consent-based model and a set of clearly-defined rights.

The consent-based model requires ongoing informed consent for the lawful processing of personal data, allowing individuals to withdraw their consent at any time. For example, in the European Union, the General Data Protection Regulation (GDPR) establishes consent as a legitimate ground for processing data, with strict requirements for it to be "*freely given, specific, informed and unambiguous*". This high threshold compels organisations to reconsider their approach to data management, influencing the landscape of data privacy disputes.

Despite being hailed as a significant advancement in data protection, the consent-based model brings its own challenges. Questions about 'consent fatigue' amongst individuals have gained prominence, which, coupled with the complexity of data processing activities, give rise to concerns about the extent to which consent today truly reflects *informed* choices. Such concerns can lead to disputes over the validity of consent, or the extent of data processing permitted under a given consent agreement. Any proposed dispute resolution mechanism must therefore cater to the deficiencies of this model.

When it comes to data subjects' rights, the GDPR encompasses a wide array of entitlements such as the right to be informed, to access, to rectification, and so on. However, these rights vary across jurisdictions. For example, the US lacks a federal-level data protection law, with states enacting their own laws, often significantly different from the GDPR. Take the case of the California Consumer Privacy Act, which did not originally include a right to rectification. Likewise, in Canada, the Personal Information Protection and Electronic Documents Act outlines data subjects' rights as principles for organisations to follow. Differing scopes of rights across nations necessitate a flexible dispute resolution method that can adapt to diverse legal contexts.

Privacy and Public Order

Data privacy does not exist in a vacuum; it operates within a dense network of broader societal interests. Harmonising data protection with considerations of public order, national security, and social welfare is essential. Central to this harmonisation is the principle of proportionality, drawn from the field of public law. This principle allows limited infringements of privacy rights for public interests, if such actions are necessary, appropriate, and proportional. Therefore, any proposed dispute resolution mechanism should permit balancing privacy rights and public interests.

Key Actors

Two central actors orchestrate the handling of personal data – data controllers and processors. Controllers are responsible for deciding how and why personal data is processed, with obligations such as ensuring lawful data processing, practicing data minimization, and implementing data security measures. Processors, on the other hand, handle personal data under the controllers' directions, with a responsibility to follow such instructions, while ensuring data security. The relationship between these actors is centred around the allocation of liability. Under the GDPR, both these players can be held liable for breaches, potentially leading to significant monetary and reputational damages. While the processors' liability is limited to violations of either the GDPR or the controller's directions, the scope of the latter's liability broadly extends to the collection, use, and disposal of personal data. Therefore, it is crucial to have in place a dispute resolution forum, which can navigate not only primary disputes between data subjects and controllers, but also conflicts that may arise between controllers and processors. Courts are unsuitable for this purpose, given that data disputes are likely to involve rights across jurisdictions, requiring resource-intensive litigation in each respective national court.

Arbitration as a Solution

Arbitration could help navigate the aforementioned challenges. To illustrate arbitration's efficacy in resolving data privacy disputes, let us consider a hypothetical scenario. Consider the case of a business-to-business (B2B) dispute involving two technology companies, Company A (U.S.-based) and Company B (EU-based). The dispute stems from a data breach concerning user data processed by Company A under a data processing agreement. The contract includes an arbitration clause with a designated arbitral institution. In this case, arbitrators well-versed in both EU and U.S. data laws would be able to facilitate a thorough assessment of the dispute. They could analyse the intricate

details of the data breach, security standards, and contractual obligations, culminating in an award based on comprehensive legal analysis, surpassing what a national court might accomplish. Furthermore, given the cross-border implications, the enforceability of the award in both jurisdictions under the New York Convention provides a crucial advantage.

In respect of both arbitrator expertise and cross-border enforceability, data protection disputes are comparable to patent or trademark infringement cases. Both these intellectual property rights (IPR), like data subjects' rights, are territorially limited due to varying legislative scopes across jurisdictions, necessitating adjudicators with expertise in the relevant laws and seamless cross-border enforcement. The UK Court of Appeal has affirmed arbitration as the most cost-effective and efficient supranational dispute resolution procedure for such cases. The confidential nature of arbitration can safeguard proprietary data and individuals' privacy, a level of protection not always available in court proceedings. Moreover, as an expeditious process arbitration can reduce the risk of exacerbated damages or lost critical evidence, unlike prolonged appeals in court litigation.

However, this hypothetical scenario also underscores certain challenges, particularly in terms of the financial implications of arbitration. While arbitration is generally more confidential and can be cost-effective compared to litigation, in the context of data privacy disputes, which are often high-volume and low-value, the costs associated with arbitration can become a significant barrier. This is especially relevant as these disputes frequently involve complex technicalities and legal nuances, potentially escalating arbitration expenses. Such financial constraints can discourage individuals from pursuing their privacy rights, emphasising the need for a more accessible and cost-efficient ADR mechanism. In light of this, the adoption of a model akin to the expert determination used in domain name disputes (i.e., ICANN's Uniform Domain-Name Dispute-Resolution Policy) could offer a more suitable solution. This approach could provide a more streamlined, less costly avenue for resolving data privacy disputes, thereby enhancing transparency, accessibility, and cost-effectiveness in the realm of data privacy arbitration, and ensuring that individuals and smaller entities are not deterred from seeking justice due to prohibitive costs.

Refining Arbitration: One Size Does *Not* Fit All

While arbitration presents a compelling avenue for resolving data privacy disputes, its framework must be meticulously refined to address the specific challenges highlighted, with a particular emphasis on the cost factor. This consideration becomes crucial in the frequent scenarios of disparity in power and resources, where individuals or smaller entities face off against larger corporations. Ensuring that the arbitration process is not only fair but also financially accessible is vital for maintaining its viability and effectiveness as a dispute resolution mechanism in the complex landscape of data privacy.

Regarding challenges posed by the multiplicity and diversity of data protection laws, arbitration can offer solutions that accommodate differing scopes of data privacy rights across jurisdictions. This can be achieved by allowing parties to appoint arbitrators who are well-versed in the diverse legal contexts inherent to a given dispute. In balancing privacy and public order, a key question is that of arbitrability. Generally, disputes based on rights *in personam* are considered arbitrable. However, data privacy disputes involve both individual rights, and layers of public interest considerations. While the arbitrability of such disputes involving both public and private interests has been a topic of debate, emerging legal trends have showcased the possibility of

accommodating such considerations with arbitration. In *Eco Swiss*, the European Court of Justice (ECJ) confirmed the arbitrability of antitrust disputes, another area that involves an interplay between public and private interests. This conclusion on arbitrability also holds true for IPR disputes, especially those involving patents. It seems plausible to extend a similar approach to data privacy disputes. By infusing public interest considerations into arbitration, the balance sought by principles like proportionality can be facilitated.

Furthermore, arbitration can help navigate complicated controller-processor dynamics. The confidentiality inherent in arbitration would allow these actors to avoid the public scrutiny of court proceedings and reputational injuries. Moreover, due to arbitration's flexibility, evidentiary hearings can occur on an expedited basis, even hour-by-hour, spanning consecutive days. Disputes arising out of the controller-processor relationship can thus be settled speedily, causing minimal strain on their business dynamic.

The Way Forward

Moulding arbitration using the above suggestions will help elevate the process as a whole. For instance, recognising the balance between private rights and public interests can promote increased transparency without hampering confidentiality, through the publication of redacted arbitral awards. Confidentiality would then no longer limit the development of data privacy jurisprudence. To enhance consistency in this rather unpredictable field, a repository of arbitration rulings on data privacy disputes can also be maintained.

Moving forward, it is important to recognise arbitration as just one part of a comprehensive strategy for resolving data privacy disputes. This approach should include both post-dispute resolution and proactive measures such as a mediation stage, acting as an early intervention to encourage amicable solutions and possibly avoiding arbitration or litigation altogether. Drafting clear agreements that define the liability-sharing between data processors and controllers also plays a crucial role in preventing potential disputes. Implementing this multifaceted approach, with an emphasis on mediation and proactive conflict avoidance, will not only facilitate more effective dispute resolution but also foster trust within the data privacy ecosystem, which is essential for ongoing innovation and growth in the digital economy.

This entry was posted on Monday, December 11th, 2023 at 8:45 am and is filed under Data Disputes, Data Protection, Digital Dispute Resolution Rules, Privacy
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.