

Data Privacy in International Arbitration

October 2018

Authors: [Dr. Markus Burianski](#)

The GDPR has cast an international spotlight on data protection due to its wide territorial scope of application and high penalties. Since arbitration proceedings will inevitably handle personal data and the legal issues arising in connection therewith are manifold, it appears wise to tackle data-protection concerns as early as possible.

Data protection in the EU has tightened

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018. Four months into its application, it is apparent that the new data protection regime in the EU imposes a range of unchartered obligations on companies processing personal data and provides rights to those individuals whose data is processed. Any violation thereof can be fined by up to four per cent of a company's annual global turnover or €20 million, whichever is higher, and can affect any company offering goods or services in the EU, irrespective of its establishment.

The vast reach of the GDPR is rooted in the definitions of processing personal data. Protected "personal data" includes simple information such as a work email address, telephone number or an IP address – anything through which a person can be identified. "Processing" is equally broad, encompassing any operation of personal data such as the organisation, use or erasure of information. The GDPR in general prohibits any processing of personal data or transferring data to non EU-countries absent a valid justification, establishing a "privacy-by-default" regime.

The GDPR provides for several exemptions, which include *inter alia*, the explicit consent by the data subject, the necessity to process personal data for the performance of a contract, or to comply with a legal obligation, or for the purpose of a legitimate interest. In practice, consent comes with the downside that it can be withdrawn at any time and contains a right of the data subject to transmit the collected data to any other company. Processing personal data for the performance of a contract, to comply with a legal obligation or for the purpose of a legitimate interest is more relevant in the context of arbitration, but requires a careful balance of the data subject's interests. The transfer of data across EU borders, a frequent phenomenon in international arbitration, is also allowed where it is necessary for the establishment, exercise or defence of a legal claim.

Complimentary to the obligations imposed on companies, data subjects enjoy wide-ranging rights such as requesting access to the personal data, access to information concerning, *inter alia*, the purpose of the processing and to whom the information has been disclosed, as well as the right to erasure. All provisions are flanked by the GDPR's underlining principles set out in Article 5, including the principle of purpose limitation and data minimization.

Implications for international arbitration

Processing of personal data in arbitral proceedings

The general prohibitions on processing and transporting personal data will inevitably affect arbitration proceedings at all stages. Even an internal review of old correspondence and documents at the outset of a dispute in preparation thereof can constitute processing personal data, the purpose of which will have to be compatible with the purpose the data was originally collected for or be covered by consent. Employees may have to be informed that their data may later be processed and transferred in arbitral proceedings. Engaging external counsel as well as correspondence with the tribunal will require a transfer of personal data possibly across EU borders. It might therefore be wise to raise data protection issues in a data-protection protocol early in the proceedings, not least to present a concept for data-protection to regulatory authorities. It could identify what data will be relevant, if there will be a transfer outside the EU and set out measures to ensure that data processing is kept to a minimal and only concerning truly relevant data.

Evidence

Obligations imposed by the GDPR might also clash with a document production order by the tribunal, as the documents will contain personal data. Although at a first glance this seems covered by the exemption “compliance with a legal obligation”, a document of an EU-advisory body on data protection¹ clarifies that the exemption only covers legal obligations created by Member State law, not ones created by an arbitral tribunal order. Relevant is, however, an exemption under “legitimate interest”. This will require a careful weighing of interests in the individual case, considering what type of data is being processed (if it is especially sensitive), their volume and possible measures like blackening the relevant documents. The principle of necessity and proportionality will also require carefully limiting document production to the extent necessary.

Expert witnesses

Another area when data protection issues can arise is dealing with expert witnesses. Although it is easy to ask for consent before involving them, consent carries the risk of a later withdrawal. Here though, the processing can fall under the exemption of “necessary for the performance of a contract to which the data subject is party”, as the personal data (e.g., the name, profession) are relevant for the meaning of the expert statement in the arbitral process.

Transfer to non-EU countries

The transfer of data into non-EU countries requires either that the European Commission has deemed the destination country able to ensure a sufficient (or an acceptable) level of protection or that the transfer falls under the exemption of “necessary for the defence of a legal claim”. The standard for necessity is high though; adequate steps are required to ensure that only relevant documents are transferred.

All of the above require strategic planning from the outset of a dispute, including for the internal investigation preceding an internal case analysis, litigation holds, the selection of arbitral institutions, the instruction of external counsel, the nomination of arbitrators etc. Companies are well advised to review their internal dispute-related processes in due time and to plan dispute-specific data protection strategies at the outset of a dispute.

White & Case LLP
Bockenheimer Landstraße 20
60323 Frankfurt am Main
Germany

T +49 69 29994

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.

¹ Art. 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross-border civil litigation.