REPRINT

CD corporate disputes

PRIVILEGED AND CONFIDENTIAL: CROSS-BORDER DIFFERENCES IN THE PROTECTION OF CONFIDENTIAL INFORMATION

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JUL-SEP 2019 ISSUE

www.corporatedisputesmagazine.com

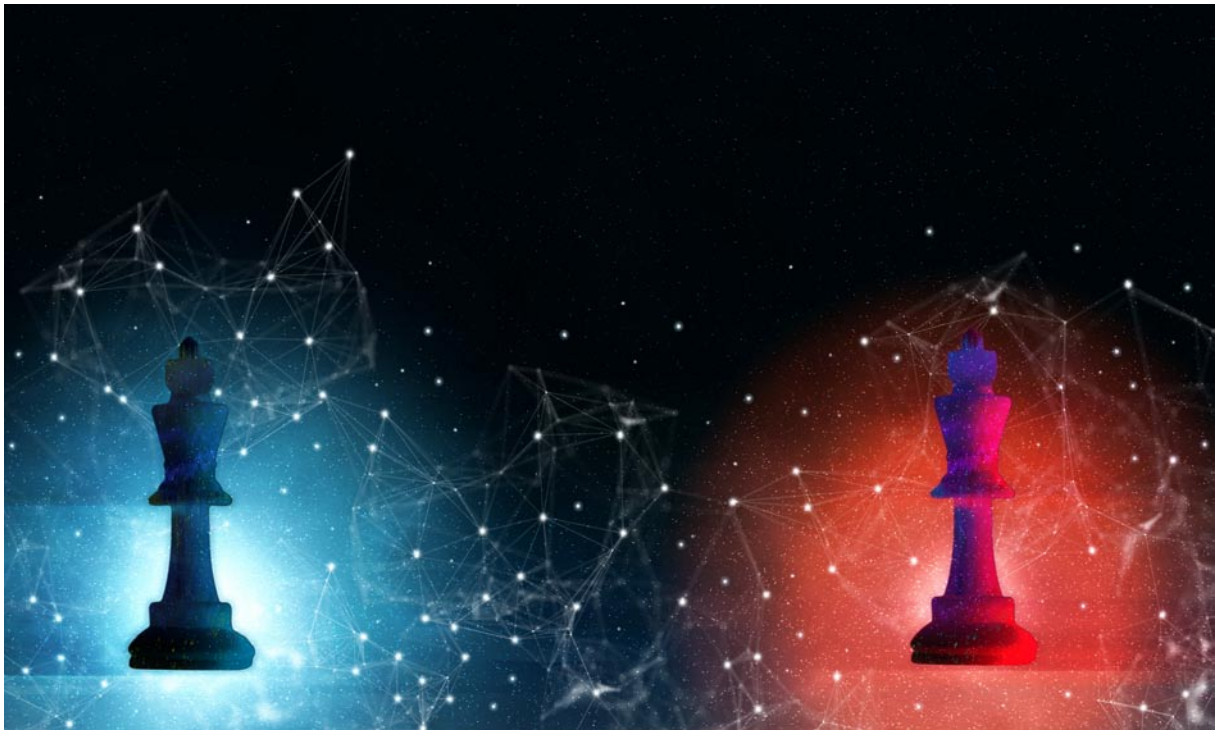
Visit the website to request
a free copy of the full e-magazine

FTI CONSULTING™

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

HOT TOPIC

PRIVILEGED AND CONFIDENTIAL: CROSS-BORDER DIFFERENCES IN THE PROTECTION OF CONFIDENTIAL INFORMATION



PANEL EXPERTS

Mark A. Lubbock
Partner
Brown Rudnick LLP
T: +44 (0)20 7851 6062
E: mlubbock@brownrudnick.com

Mark Lubbock is a partner in Brown Rudnick's intellectual property group. He specialises in commercial technology and privacy law. He advises clients on a wide variety of both contentious and non-contentious matters and has extensive experience in the intellectual property, data protection, information technology, healthcare, e-commerce, outsourcing, and commercial contracts practice areas.

Désirée Prantl
Principal Associate
Freshfields Bruckhaus Deringer LLP
T: +43 (1) 515 15 0
E: desiree.prantl@freshfields.com

Désirée Prantl specialises in international dispute resolution. She focuses on complex disputes in the construction, energy, finance and technical sectors and has resolved disputes arising out of complicated contractual relationships. Her practice involves vast experience in national and international data protection regimes and compliance thereof. She is admitted to the Austrian bar and speaks German, English, French and Italian.

Brian Stuart
Senior Managing Director
FTI Consulting
T: +44 (0)20 3727 1706
E: brian.stuart@fticonsulting.com

Brian Stuart works with clients by using his international expertise and significant experience in methodologies and technology solutions, to help them tackle issues such as AML, banking insolvency, bribery and corruption, sanctions breaches, cyber breach investigations and competition abuses. He has specialised in working with multinational organisations to set up and effectively manage large cross-border e-discovery exercises across a number of jurisdictions.

William Ridgway
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
T: +1 (312) 407 0449
E: william.ridgway@skadden.com

William E. Ridgway is a former federal prosecutor and is an experienced trial and appellate lawyer whose practice focuses on cyber security and data privacy matters, white-collar crime and intellectual property litigation.

CD: How does the current data privacy landscape present challenges for cross-border confidentiality?

Lubbock: Within the European Union (EU), the data privacy landscape is governed by the General Data Protection Regulation (GDPR), whereas rights of confidence in information, which may or may not be personal data, are governed by the laws of Member States which have or will be, to some extent, harmonised by the requirements placed on Member States by the Trade Secrets Directive. Confidential information may include personal data and some personal data may be confidential. A challenge which many organisations face has been caused by the failure to appreciate the important distinctions between the two and the rights and obligations associated with each. This can be exacerbated in cross-border transfers where the transfer of personal data is heavily regulated, whereas the transfer of confidential information, which is not personal data, is generally not.

Ridgway: The increased focus on data privacy poses a significant challenge to the bounds of cross-border transfers in US litigation and in other jurisdictions. Emerging data privacy regimes in the EU, Asia, Latin America and even some US states, complicate and in some circumstances bar, the transfer of data across borders in connection with a legal proceeding. The prospect of conflicting obligations is heightened, moreover, with passage of new extraterritorial production laws, such as the US's Clarifying Lawful Overseas Use of Data Act (CLOUD Act) and the UK's Crime (Overseas Production Orders) Act (COPO Act). Courts in the US and elsewhere will continue to wrestle with these overlapping legal regimes, balancing the need to facilitate data transfers against the need to protect personal privacy.

Stuart: The attention surrounding the GDPR has brought privacy to the foreground of planning any matter involving a cross-border transfer of data. What was once a nod to privacy, the phrase 'it is the company's information or asset' was enough to permit the transfer of data. Now, there needs to be a proper plan put in place and we, as the collectors and processors of data, are expected to have the ability to identify personally sensitive and identifiable data, protect information and redact it at a much earlier stage in the lifecycle of an e-discovery exercise. We would not contemplate the transfer of data without an explicit agreement stating why we are transferring the data, to whom and how.

Prantl: The current data privacy landscape has been 'shaped' by the globalisation of business. New digital technologies with enhanced capabilities have increased the risk of unauthorised data disclosure. This has spurred significant privacy

law developments in Europe and elsewhere. For instance, the GDPR in the EU, which celebrated its first anniversary on 25 May 2019, has created momentum and led to amendments of local data protection laws across many other jurisdictions. Notably, new privacy laws were adopted in the US, through the California Consumer Privacy Act, and Brazil, through the General Data Protection Law, both of which will come into force in 2020. India has introduced a new wide-ranging data protection bill. As a Russia particularity, data localisation rules require the accumulation, storage and processing of personal information of Russian citizens on servers located within Russian borders. Undoubtedly, differences in data protection laws, as well as the dynamic nature of the data privacy landscape, have presented challenges for cross-border confidentiality. However, recent developments show a harmonising effect of the GDPR far beyond European borders.

CD: With cross-border data transfers frequently required during commercial dispute resolution processes, are you seeing an uptick in instances where privileged or confidential information is breached?

Ridgway: Data is most at risk when it is on the move, and cross-border data transfers by their very nature involve the movement of massive amounts of sensitive data from one party to another, often via multiple intermediaries. These productions are attractive targets for hackers, as cyber security experts have noted. It is difficult to assess whether there has been an uptick in the number of successful attacks, in part because it can be challenging to trace back a breach to a particular data repository, but there has certainly been an increase in the number of attempted attacks. As has been widely reported, one notable point of vulnerability is law firms, which often store or have to access these sensitive data productions. Indeed, according to the American Bar Association, one out of every four law firms has been the victim of a data breach.

> **"The increased focus on data privacy poses a significant challenge to the bounds of cross-border transfers in US litigation and in other jurisdictions."**
>
> *William Ridgway,*
> *Skadden, Arps, Slate, Meagher & Flom LLP*

Stuart: The need to secure client data in transit has always been paramount. It is imperative that it is a well-planned transfer and that data is securely safeguarded by means of encryption at the data, container and physical media level. We are not seeing an increase in breaches, but we are seeing a stronger effort put on identifying personally sensitive data before being transferred. Technology can help secure data in transit and can help protect sensitive data, but only when used with care and skill. There are measures that can be taken to make any breach of data evident. When transferring data on physical media, the media should be kept in tamper evidence sealed security bags. Human error also plays its part in contributing to data breaches where key parties, under time pressure, fail to check the items they are disclosing to adversarial parties only to find they include client names and details.

Prantl: Recent experience shows that increased cross-border data transfers have not led to a considerable uptick in breaches of data protection regimes. There are two possible explanations for this phenomenon: either companies' awareness of the severe consequences faced in the event of non-compliance with existing data protection frameworks has increased, or sanction systems are being circumvented or are failing to spot violations. Currently, when commercial transactions, as well as disputes, involve confidential information, parties are more frequently pointing to such circumstances and related concerns. As a result, special confidentiality agreements are often concluded. Such agreements increase awareness and diligence in terms of compliance with the tailor-made data protection regime on both sides. Thus, breaches are less likely to occur. Moreover, parties may agree on exemptions allowing cross-border data transfers of confidential information or parties may give their explicit consent to such transfers.

"Recent experience shows that increased cross-border data transfers have not led to a considerable uptick in breaches of data protection regimes."

Désirée Prantl, Freshfields Bruckhaus Deringer LLP

Lubbock: We have not seen an uptick in breaches of late. A breach of privileged or confidential information in cross-border disputes usually occurs where different protections apply to confidential or privileged information across different jurisdictions.

For example, in Germany, unlike in the UK, a prosecutor is able to compel the production of privileged documents in the context of a criminal investigation. A UK company under criminal investigation in Germany which makes privileged material available to its German lawyers might be exposing itself to the risk of such material being seized by a prosecutor. Prior to a cross-border transfer, legal advice should always be sought from local counsel regarding the extent to which confidential information is protected in the recipient jurisdiction, so that any risks arising from different national rules can be managed.

CD: What specific factors need to be addressed when transferring confidential information across borders? How can parties determine what information is vulnerable?

Stuart: When dealing with a cross-border data transfer, you first need to define the roles played by the various parties in the transfer of data. A contract needs to be in place defining parties as either a controller or a processor. The key questions to ask about your own role in the transfer of the data is whether you are simply operating on instructions from lawyers or you are determining the means and purpose of the processing and review. In terms of detecting personally identifiable information (PII) inside documents, there are many libraries of terms that can be used to help locate PII terms for redaction. A challenge arises when handling items, such as a scan of an application form. Only if the scanned items are subjected to optical character recognition (OCR) can automated PII detection tools operate in those cases.

Lubbock: When transferring confidential information across borders, there are a number of factors which should be considered. Parties must consider whether the applicable data privacy laws in the jurisdiction transferring the data have been complied with and whether the applicable data privacy laws in the jurisdiction receiving the data have been complied with. Parties must also consider the level of protection afforded to the confidential information by the laws in the recipient jurisdiction. It is also important to consider whether it is necessary to put in place an agreement between the transferor and the recipient setting out their respective rights and obligations in respect of the confidential information, for example a non-disclosure or confidentiality agreement or, in respect of privileged information, a common interest or limited waiver agreement. Parties must also consider whether the recipient has appropriate technical safeguards in place for the protection of confidential information. In terms of identifying vulnerable information, the transferor should ensure that it is aware of the nature of the confidential data being transferred, and, in particular, whether the data contains any

particularly sensitive material, such as privileged information, commercially sensitive information or special category personal data. The transferor should then seek legal advice on the extent to which different categories of confidential material is protected in the recipient's jurisdiction, so it can take an informed view on the risks associated with the transfer.

Prantl: First and foremost, parties should examine if, or rather which, specific contractual restrictions or requirements regarding confidential information apply. In addition, varying landscapes of data protection laws should also be considered. To ensure a common understanding of the scope of data protection obligations, parties are well advised to contractually lay down clear terminology of the relevant terms. Nevertheless, in practice, vague terms for confidential data are often used. Expressions like 'information deemed confidential by one of the parties' or 'deemed confidential by a diligent person' provide leeway for interpretation. Instead, clear language should be used in order to avoid potential sources of dispute. Still, penalties in the event of a breach of a confidentiality agreement shall be agreed *ex ante*.

Ridgway: Both parties must ensure the confidentiality, integrity and resilience of data processing and hosting systems, and that may require instituting an approved certification

mechanism to demonstrate advanced security implementation, such as ISO 27001, a globally recognised standard for the establishment and certification of an information security management system. Another way for parties to address these issues is through an effective e-discovery protective order that creates access controls, including password protection, viewing restrictions and encryption for data and documents subject to disclosure, as well as rules for data retention, destruction or return. Such orders may also limit vendor and other third-party access to, and treatment of, e-discovery data.

CD: In your opinion, what are the essential elements of an effective cross-border data protection solution?

Prantl: It is essential that parties identify the applicable data protection laws and analyse specific data privacy constraints thereof. In case of legal constraints, for instance the limitation of international cross-border transfers of personal data, analysis of technical and organisational measures of the transfers ought to take place in order for the parties to ensure compliance. Effective measures include sending personal data by courier or by encrypted email. Sometimes there are other information requirements such as the duty to provide details on who, when, where and how the data is going to be processed. However, exemptions from these requirements may apply because of a duty of confidentiality. Effective cross-border data protection lacks a 'one-size-fits-all' solution and requires a 'tailor made' approach for every transaction or dispute instead.

Ridgway: Data protection legislation will, and in many cases already has, necessitated new requirements for cross-border data transfers. As a threshold matter, companies must now design and document more stringent methodologies and security measures, in line with newly codified accountability and data minimisation principles. When the need for cross-border data transfer arises, a cross-departmental, cross-functional team should be used to evaluate the legal and security requirements. These transfers also often necessitate the assistance of a vendor with expertise in data hosting and transfer.

Lubbock: The GDPR prohibits cross-border transfers which result in personal data being exported from the European Economic Area (EEA), except in the circumstances specified in the regulation. It is essential that parties get these data transfers right. This is not always straightforward, however, particularly for transfers from EU processors to non-EU controllers or non-EU sub-processors. For cross-border transfers within the EU, it is recommended that parties have a formal data sharing agreement in place to identify the legal

basis for the transfer and to ensure that the rights of the data subjects involved will be protected in a transparent and accountable manner.

Stuart: Businesses that want to operate efficiently across borders will want to invest in a comprehensive information mapping exercise. Having the best and most comprehensive solution for cross-border data protection is pointless, unless there is a clear sense at the top of the organisation as to why you want to govern your cross-border information flows. If all you want is a policy, so that you can say you have one, there will be many willing software providers providing a solution online. The reality is that little will be achieved without a proper tone from the top and embedding good information management principles into the culture and behavioural norms of the organisation.

CD: What steps should be taken to manage the data transfer process to ensure it complies with applicable legal and regulatory requirements?

Ridgway: As global businesses move more of their data to the cloud, this often complicates the evaluation of a proposed cross-border data transfer. In some cases, companies may not even be aware of the location of their data. To avoid the pitfalls that come with cloud-based data transfers, it is important for the legal team to work closely with information technology staff and any outside vendor to understand precisely how the data will be securely collected and transferred.

> **"The GDPR prohibits cross-border transfers which result in personal data being exported from the European Economic Area (EEA), except in the circumstances specified in the regulation."**
>
> *Mark A. Lubbock, Brown Rudnick LLP*

Lubbock: For personal data, parties need to comply with the requirements of GDPR. For confidential information, from a UK law perspective, it is important that the disclosures are subjected to well drafted non-disclosure or confidentiality agreements to ensure that the parties involved know their rights in respect of the use and disclosure of such information. In addition, depending on the technologies involved, there may be other regulatory restrictions with which to comply, such as obtaining

an export licence, which is particularly important for the export of military grade technology, for example.

Stuart: When transferring personal data from within the EEA to outside the EEA, or from a location governed by GDPR to a location not governed by GDPR, then you are making a restricted transfer. To determine if you can make the transfer data compliant, you should take appropriate legal advice to answer the following questions. First, are you transferring the data to a covered country? The list of covered countries includes those which are a member of the EU, the EEA and those where a legal framework is in place to provide an 'adequate provision' of data privacy and protection. Second, is the transfer covered by adequate safeguards? There needs to be a binding contract between the parties setting out roles and responsibilities for protecting individuals' rights and what happens in the event of any breach. Third, do you have the individuals' specific and informed consent to make the transfer? Consent has limited uses as the basis for making a transfer compliant as it can be both withheld and withdrawn at any time. There is an exception to consent arising in the circumstances where a transfer is necessary to determine if a party has a legal claim. Finally, is the data you are transferring defined as personal data and can you identify an individual from the data?

Prantl: Companies should implement internal data protection policies, as well as guidelines for employees. Compliance with policies and guidelines also requires companies to provide an adequate organisational and infrastructure framework. It is the company's responsibility to implement measures, such as encrypted communication and data transfers. It may also be helpful to appoint a chief compliance officer whose duty is to ensure internal and external compliance with data protection policies and regulations, as well as to keep the employees informed.

CD: Drilling down, are you seeing increased use of tools such as encryption and containerisation in protecting privileged and confidential information for commercial disputes? What other methods are being deployed?

Prantl: We are definitely seeing increased use of encryption and containerisation. Most notably, email encryption is being used more to ensure that content is not read by anyone other than the intended recipient. Another tool being increasingly employed by companies is limiting the number of people or entities that have access to data. Moreover, there is an increased use of 'clean teams' who are assembling, reviewing and examining confidential and sensitive data. These teams carry out their work prior to regulatory approval or the

conclusion of a deal and they must comply with certain protocols. Other methods used in practice are sending data by secure file transfer electronically or sending a locked USB stick and providing the password separately.

Stuart: We are seeing more use of encryption and containerisation tools to safeguard data, be it personally identifiable data or commercial business records. We are also seeing an increase in the use of automated redaction tools to block out personal data at the time of transfer. The use of all these tools must be well planned and tested. Stories of incidents where human error allowed data that was thought to have been secured by redaction, ended up being breached and causing embarrassment, along with a liability, attract much unwanted attention.

Lubbock: We are seeing an increase in the use of tools such as encryption, which is commonly used to protect confidential and privileged information in a number of scenarios, such as where a client transfers large quantities of electronic documents to external counsel for evidence gathering and review purposes, or where documents are disclosed to another party to the dispute or to a regulator. Encryption mitigates the risk of the data being accessed by a third party while it is being transferred from one party to another. Data rooms also offer significant levels of security. Other safeguards being employed to protect privileged and confidential information include the use of secure file transfer or file-sharing platforms to transfer data from one party to another, and the use of third-party document management platforms to ensure that the data collected from the client is stored in a secure environment, accessible only by the case team.

> **"We are seeing more use of encryption and containerisation tools to safeguard data, be it personally identifiable data or commercial business records."**
>
> *Brian Stuart, FTI Consulting*

Ridgway: Technology capabilities are maturing, and many tools, such as encryption, are becoming standard. Most of the key security measures are implemented by an outside vendor, so it is important for companies to focus on security when selecting their vendor. Working with trusted vendors that have security certifications can help ensure that

the data is secure, encrypted at rest and in transit, subject to regularly scheduled security audits and vulnerability scans, and monitored continuously for suspicious activity. Even the most extensive security measures, however, are for naught if a hacker steals the credentials of a user. In that regard, training and access restrictions, including multi-factor authentication, are essential.

CD: How do you expect cross-border confidentially issues to develop in the years ahead? Are there any particular challenges or complications on the horizon?

Stuart: With uncertainty around Brexit, if the UK ends up negotiating new trading agreements with non-EEA countries, access to personal data could become a bargaining chip used by us or against us. We are also seeing more US states adopt their own versions of a privacy act. Many of these mirror GDPR to some degree, but mainly focus on the security of data and breach notifications. Companies such as Google, Facebook, Amazon, Netflix and Apple already know everything about you from where you go, what you buy, what you are like and which other groups of people hold similar views to you. We adopt new technologies rapidly, far more rapidly than the laws of privacy can keep pace with. There is one certainty: chief executives need to get their legal, business, IT, marketing and HR leadership teams working together. The problem of information governance looks vast, but perhaps the most challenging problem to solve is getting those business functions to collaborate.

Lubbock: Regarding confidential information, the trade secrets directive will assist in ensuring the effective protection of rights of confidence in the EU. The directive requires Member States to harmonise their laws to give confidential information protection. The effect in the UK will be slight, but other Member States may have to implement laws giving greater protection to confidential information.

Ridgway: US courts will continue to examine the breadth of permissible cross-border data transfers and balance it against the need to protect personal privacy. In one of the first cases involving the GDPR since its enactment, Microsoft argued that retention and production of data relevant in a patent infringement case 'raises tension' with the GDPR and would require burdensome steps to anonymise the personal data. Yet the court in that case ordered retention and production, finding that the benefit of the data, which was relevant and proportional, outweighed the burden or expense of compliance. That ruling underscores the challenge that companies will continue to face when operating under overlapping, and sometimes conflicting, legal obligations.

Prantl: Cross-border confidentiality issues are a 'hot topic' that will gain importance in the future. As more information is exchanged across borders in the coming years, we expect to see growing awareness and concern regarding data protection. Accordingly, the trend of introducing new data protection regimes is expected to continue. Streamlined and harmonised regimes will not only facilitate cross-border transfers, but also decrease the number of breaches which occur as a result of misunderstandings or lack of awareness. A relatively new issue concerns trade secrets. EU member states had to adopt laws and administrative provisions in order to comply with the Trade Secret Directive by 2018. The Directive regulates unlawful acquisition, disclosure and use of trade secrets. This, in turn, is related to another issue: the need for data protection against the opposing party, which, in many cases, is the competitor. Furthermore, it is important to emphasise that the culture of a country has a great impact on the highlighted issues. A good example is Scandinavia, where people are generally less sensitive to greater disclosure of personal information. CD