Client Alert: Data Transfers and Investigations

Date : September 8, 2020

We first published this note on 10 August 2020 but we've added more details on the Aven case below and on the collapse of the Swiss Privacy Shield scheme.

In July we looked in some detail at the European Court's ruling in the latest instalment of the Schrems v. Facebook litigation (see https://bit.ly/pshielddead). Since then the equivalent Swiss Privacy Shield scheme has also collapsed (see https://bit.ly/swisspshield). But was does this mean for investigations?

What's the issue?

Increasingly organisations are being required to conduct investigations to meet their legal obligations. The duty to investigate arises in different laws around the world including the UK Bribery Act 2010 (see https://www.corderycompliance.com/uk-bribery-act-2010-faqs/) and the French Sapin II law (https://www.corderycompliance.com/france-adopts-new-sapin2-anti-corruption-law/). Changes are also contemplated in other countries including Germany.

These investigations happen around the world and multinational organisations will often want to transfer data between various locations and its investigators, management or regulators in other countries. The situation is made more challenging by the large volumes of data involved in modern day investigations. For example the recent Airbus investigation (see http://bit.ly/busbribe) involved the collection and analysis of more than 30 million documents.

One of the most challenging areas for multinational businesses has been a heightening of the conflicts already felt between data protection laws and the requirements imposed by bribery legislation. The fact that, in basic terms, in some corruption laws the burden of proof is reversed and the company will have to prove that it took adequate procedures to avail itself of any defence, rather than the prosecution prove that it did not, has increased the focus on these internal procedures.

Data protection law has been strengthened too. The coming into force of the General Data Protection Regulation (GDPR) in May 2018 has already made these conflicts more acute (see www.bit.ly/gdprfaq). Additionally in May 2018 the UK introduced new data protection legislation, the Data Protection Act 2018 (DPA 2018), which has additional criminal offences that could be committed for example in the course of a bribery investigation (see http://bit.ly/ukdpa2018).

These conflicts are significant and this note gives a simplified version of some of the issues. It uses data protection specific terms which are explained here www.bit.ly/gdprwords. It is important to stress however that in most cases specialist legal advice will be required to balance the various risks involved.

What does GDPR say?

GDPR imposes obligations on organisations to process data fairly and lawfully. It also has specific principles which must be followed when transferring data outside of the EEA which are outlined in Chapter V of GDPR. Transfers are only permitted when there is a lawful basis for the transfer. That could include:

1. An adequacy decision (such as the decision authorising Standard Contractual Clauses (also known as Model Terms or SCCs))
2. Binding Corporate Rules
3. Consent from the individual whose data is being transferred

Consent rarely works in an investigation. There are a number of detailed reasons why this is the case, amongst them the fact that it is hard to get valid consent from an employee and that even then consent can be withdrawn. If an individual withdraws consent that is likely to cause difficulties further down the line in an investigation especially

if a regulator or prosecutor asks to see the data.

It is also important to remember that the data collected in investigations is often special category data under GDPR (the rough equivalent of sensitive personal data under pre-GDPR law). GDPR Art. 9 defines special category data and the GDPR regime gives that data extra protection. GDPR also gives extra protection to criminal data which is covered by GDPR Art. 10. It is important to remember that criminal data includes data relating to the suspicion of a criminal offence which again is the type of data frequently gathered in any investigation.

What about data subject rights?

It is also important to remember that GDPR imposes a number of other requirements which could also have an impact on investigations. These include (subject to some exceptions):

1. A right for someone involved in any investigation to have their personal data handled lawfully (GDPR Art. 6)
2. A right to be provided with information about the way in which personal data is handled (GDPR Arts. 13 & 14)
3. A right to see the personal data an organisation holds on them (GDPR Art. 15)
4. A right to rectify the data held (GDPR Art. 16)
5. A right to be forgotten (GDPR Art. 17)
6. A right to restrict processing (GDPR Art. 18)
7. A right to object to some forms of data processing (GDPR Arts. 21 & 22)
8. A right to be informed of any data breach where that might result in a high risk (GDPR Art. 34)

Individuals who are the subject of investigations are using their rights. For example in the Guriev case in 2016 two individuals (both Russian nationals) successfully used data protection law to request details of the investigation into their business affairs being conducted by investigators appointed by a former business partner involving transactions in Russia and Cyprus (see here https://www.corderycompliance.com/subject-access-requests-and-investigations/).

Anyone who is harmed by an investigation into them can also sue for a breach of data protection law. This happened in a case where judgment was handed down last month, Aven v Orbis Business Intelligence Ltd. This case involved litigation under the Data Protection Act 1998 (the UK's pre-GDPR data protection law) over the Trump Russia dossier prepared by former intelligence agent Christopher Steele and his firm, Orbis. In this case two of the individuals named in the dossier (of Russian or Ukrainian origin) recovered £18,000 each for a breach of their data protection rights. You can read our summary of this case here https://bit.ly/avenorb.

In extreme cases a court or a Data Protection Authority could also order an investigation to stop and/or issue a fine against those conducting the investigation. A regulator or prosecutor may also express concerns if the way in which data has been collected means that they could not take subsequent action. That could also mean that a Deferred Prosecution Agreement would not be available as a way of dealing with the case.

But what about the exceptions?

As we've said already some exemptions (known as derogations) exist for data transfer by way of GDPR Art. 49. In addition to consent those exemptions include where:

1. The transfer is necessary for important reasons of public interest.
2. The transfer is necessary for the establishment, exercise or defence of legal claims.

Member states can add to these derogations if they wish. It is important to remember however that these exemptions are mostly built around necessity. As we have said before (for example in our alert on the data protection aspects of the pandemic www.bit.ly/gdprvirus) necessity goes beyond convenience and the burden of proof will be on the transferring party to prove that it is necessary. This is likely to be a difficult hurdle to get over particularly in an investigation where the consequences for individuals could be severe. The burden of proof point was also emphasised by the judge in the Aven case.

There are additional exemptions and qualifications to the data subject rights outlined above but again detailed consideration will be required when limiting those rights. This is an area where specialist advice will be required. In general terms however the exceptions are not as wide as they might appear, as the Guriev case shows.

What about privilege?

The rules on privilege vary from country to country and just because a law firm commissions an investigative report does not necessarily mean that it would be privileged (in fact a law firm commissioned the report in the Aven case involving the Trump Russian dossier). However, a properly scoped and properly conducted investigation led by external counsel can attract privilege and that is likely to be worth considering given the prospects of litigation and the fact that privileged data is treated differently under data protection law.

How does the new case ECJ ruling make the situation more challenging?

The ECJ's ruling makes the situation more challenging as Privacy Shield, relied on by some to conduct investigations, including some external law firms, is now effectively dead. The other main way or legitimising these data transfers, SCCs, remains but using SCCs becomes more challenging. As a minimum the organisation transferring data will need to do due diligence not only on the recipient but also the countries that the data might travel to. There will be special concerns when transferring any data to the US given what the ECJ said about the lack of legal protection for personal data in the US.

Is this just an EU-US thing?

The simple answer is no. Whilst the EU-US Privacy Shield only covered transfers from the EU to the US SCCs were used to legitimise transfers from the EU to many other countries. Whilst the ECJ's ruling principally concerns data transfers to the US following the same reasoning other countries, including Russia and China, will also be problematical for data transfers. Any transfer outside of the EEA could be problematical as many jurisdictions have laws which allow the security services and others to look at data.

In addition to the EU-US Privacy Shield a similar scheme was in place for transfers from Switzerland. This scheme has also now collapsed (see https://bit.ly/swisspshield).

It should also be remembered that many countries including those in Asia Pacific, Canada and South America also have legislation to protect data. It is usually necessary to look closely at the specifics of the law in the jurisdictions that you are dealing with and to understand where interviewees or suspects reside and how their data is processed.

Data export laws

In addition to data protection law, some countries (such as France, Switzerland, China and Russia) have restrictions on the data that can be transferred from that country. These laws are generally separate from data protection legislation and will require a separate analysis. In some cases consent (even if you can obtain valid consent) will not solve the problem.

What about criminal offences?

Care should be taken to avoid the criminal offences contained in DPA 2018 if the investigation touches the UK. DPA 2018 contains a number of criminal offences which could be committed whilst conducting an investigation including:

- s.170 – an extended offence of unlawfully obtaining data or refusing to return it when the data controller asks for it back. An offence under s.170 could be committed for example when an investigator receives data from a third party (such as a travel company) and then refuses to give it back if it is requested to do so;
- s.171 – a new offence of re-identifying anonymised or pseudonymised data. This could include an investigator trying to work out the identity of an individual from IP addresses or CCTV images;

- s.173 – a new offence of altering data to prevent disclosure to a data subject after a data subject makes a request under GDPR or DPA 2018.

There are various defences in DPA 2018 to these new offences. One of the defences to a s.173 prosecution could be that the "alteration, defacing, blocking, erasure, destruction or concealment" of the information would have occurred even if a data subject request had not been made. This should mean that in some circumstances routine data housekeeping would not attract a criminal penalty, although organisations will want to put measures in place to ensure that they comply with the law when receiving a valid request. On conviction under s.170 the court could order documents to be confiscated.

What can you do to reduce risk?

For most organisations, removing risk in this area is simply not achievable. They will need to conduct investigations and sometimes that could involve them compromising their compliance with other laws. Historically many organisations have taken the view that, since FCPA and other bribery fines outweigh data protection fines, their data protection compliance would give way. Since GDPR includes theoretical penalties of 4% of annual revenue, that equation is not now as simple.

Organisations will want to have measures in place to reduce their risk which will likely include:

1. Doing a data protection impact assessment prior to starting the investigation to look at the ways in which data is likely to be handled and how risk can be reduced.
2. Doing due diligence on providers – including external counsel – and looking closely at how they intend to handle data.
3. Reducing data transfers where possible. This might involve (where possible in the current crisis) moving investigators to the data rather than moving data to the investigators.
4. Looking at the six principles in GDPR in detail. For example can searches be constructed to look proportionately at data in stages rather than gathering all of the data and moving it to a server hosted outside the EEA?
5. Consider approaching the regulator or prosecutor if the investigation is responding to a specific issue. Some regulators and prosecutors are alive to data protection risks particularly since it is rumoured that at least one trial in the UK has collapsed due to data protection issues not being handled correctly. If you can explain the situation and your concerns properly it could be that the investigation can be configured differently. In some cases it can be safer for a prosecutor or law enforcement agency to get the data than it is for a private organisation.
6. You could consider approaching a Data Protection Authority or a court for assistance. A Data Protection Authority cannot permit the transfer but it can indicate that it may not take action. A court could permit the transfer. An approach to the court was made for example in the Madoff investigation in 2009 to authorise the transfer.
7. Consider if anonymisation is possible. From our experience whilst pseudonymisation can be a possibility the cases in which useful data can be anonymised in an investigation are few and far between. Anonymised data is not subject to GDPR but pseudonymised data is. If you are anonymising or pseudonymising data, bear in mind the criminal offences that exist in DPA 2018 for reversing that.

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com