New EU Opinions Clarify Data Privacy and Third-Country Data Transfer Laws While Setting the Stage For More Regulation

Summary

The European Commission (the “Commission”) and its Article 29 Data Protection Working Party (the “Article 29 Committee”) have published new opinions expressing concern about compliance with EU privacy law applying to transfers of data outside the European Union (“EU”). Taken as a whole, the opinions point toward greater EU scrutiny of data security practices and further regulation of data transferred to and from the EU.\(^1\)

Early in 2006, the Commission signaled its strong preference for more widespread reliance on the stringent privacy protections contained in its standard contractual clauses, which have been widely criticized by companies as being impractical in many real-life business situations involving trans-Atlantic data transfers.\(^2\) In response, the Commission is considering whether to impose more stringent reporting on cross-border data transfers, a move that could have a chilling impact on commercial data flows to the US.

The Article 29 Committee has issued opinions pushing back against new EU rules requiring telecommunications providers to retain traffic data for law enforcement purposes.\(^3\) The Article 29 Committee also issued an opinion narrowing the basis upon which Internet Service Providers (“ISPs”) and Email Service Providers (“ESPs”) can scan the content of emails and attachments.\(^4\) Here, the Article 29 Committee found that anti-virus and anti-spam software was justified under both the “e-Privacy Directive”\(^5\) and the “Data Protection Directive,”\(^6\) but only if the confidentiality of emails and attachments is maintained and there is no scanning for predetermined content without specific authorization. The Article 29 Committee expressly warned that any person

---

1. For the purpose of this advisory, the term “EU” refers not only to the 25 Member States of the EU but to all other countries in the European Economic Area (EEA) covered by the Directives mentioned, which include Iceland, Liechtenstein, Norway, the Channel Islands, and the Isle of Man.


using email scanning and data transfer programs such as “Did they read it?” software, which allows the sender to track the usage and onward transfer of an email without the recipient’s knowledge, on EU-related data would violate EU law.

The Article 29 Committee also addressed simultaneous compliance by publicly traded companies with the whistleblower requirements of Sarbanes-Oxley legislation (“SOX”) 7 and existing EU data privacy law, setting out general guidelines on how whistleblower schemes can be made compliant with EU data security law. The Article 29 Committee encourages using confidential, versus anonymous, reporting and establishing additional protections for the accused. 8 As discussions between the EU and US government on this subject are ongoing, it is expected that more concrete and binding requirements will be issued in the near future.

Finally, both the Commission and Article 29 Committee have commented on the recent decision by the European Court of Justice (the “Court”) that annulled the existing agreement between the EU and US to share certain airline passenger data in an effort to prevent terrorism. 9 While a new agreement will likely be created shortly, a disagreement between the Commission and the European Parliament over the types of personal data to be transferred and the adequacy of data security could lead to additional litigation.

**Using Standard Contractual Clauses for “Third Country” Data Transfers**

On January 20, 2006, the Commission issued a “Staff Working Document” on the status of standard contractual clauses used to ensure the security and privacy of personal data transferred from the EU to non-EU countries (“third countries”). 10

In 2001 and 2002, the Commission adopted two decisions that provided standardized language to help facilitate the safe transfer of personal data. 11 In 2004, the Commission also approved a list of business-specific standard contractual clauses, 12 which were designed to be more efficient but which businesses have found difficult to apply. However, the Commission has taken the lack of records on the use and effectiveness of such clauses to imply that personal data is not being adequately protected, and if standard contractual clauses are not more widely utilized it is likely that additional reporting requirements may result. Indeed, the Commission is already

---


8 The opinion is limited to accounting, internal accounting controls, anti-bribery, auditing matters, or banking or financial crime issues.


10 Data Privacy Directive, 1995 O.J. (L 281). Under the Data Privacy Directive, transfers of personal data from an EU member state to a third country may only take place when: (1) the subject of the data unambiguously agrees to the transfer; (2) the Commission has made an “adequacy finding,” whereby pursuant to Article 25(6) of the Data Protection Directive the Commission assesses the third country’s domestic law or other international commitments as relate to protection of individual privacy rights; (3) the transfer is authorized under one of the derogations listed in Article 26(1) of the Data Protection Directive; or (4) the data exporter and importer have drafted a contract, utilizing either ad hoc language or one of the standard contractual clauses developed by the Commission, to guarantee adequate data security.


12 The business clauses are published at 2004 O.J. (L 385) 74-84.
considering consolidation of the business clauses with its other standard contractual clauses into a single instrument that would also include a standardized procedure for depositing copies of such contracts with EU Member States.

The Commission continues to encourage companies to use standard contractual clauses as an alternative to the derogations provided for in Article 26(1) of the Data Protection Directive, as contractual clauses provide greater control of data once it leaves the EU for a third country and potentially beyond. The Commission is concerned that current data protection law does not cover data that is forwarded by an approved third country data recipient on to another party not covered by the initial contract. The Article 29 Committee is currently investigating this loophole and further regulations are likely.

The Commission also stated that:

- Standard contractual clauses must be modified to reflect the requirements of a particular transfer.
- While the Commission does not object to the subscription of standard contractual clauses by several data exporters or importers as a group, the information provided should be at the same level of clarity and specificity that is required for a single data exporter and a single data importer.
- Parties utilizing standard contractual clauses must be prepared to supply an authenticated copy of the contract in the national language of the requesting EU member state.

### Data Retained from Publicly Accessible Networks for Law Enforcement Purposes

Opinion 3/2006, adopted March 25, 2006, is the Article 29 Committee’s response to concerns about the European Council’s Directive that traffic data from publicly accessible communications networks can be retained for the purpose of combating serious crime. The Directive has proved controversial and unevenly applied by EU Member States and the Article 29 Committee calls for more safeguards to protect the “vital interests of the individual,” in particular the right to confidential electronic communication.

To narrow the impact on privacy of the new data retention rules, the Article 29 Committee opinion found that under EU law:

- Public electronic communication service or network providers may not process data retained for public order purposes.
- Systems for storing data retained for public order purposes should be separate from those systems used for ordinary business purposes.

---


Minimum technical and organizational security measures should be developed though the Article 29 Committee does not specify what those standards should be.

The amount and type of data to be retained should be minimized, though the Article 29 Committee provides no details.

Only select police authorities may be granted access to retained data, with a list of authorized parties made public and logs kept by supervisory authorities to ensure effective oversight.

Access to retained data should be authorized by judicial authorities on a case-by-case basis, though additional access may be allowed in those countries where authorized by law.

Law enforcement agencies are not allowed to engage in large-scale data mining of the travel and communication patterns of people unsuspected by law enforcement authorities.

Email screening services

Most ISPs and ESPs use anti-virus and anti-spam filtering tools to protect their networks and servers, and in more limited cases to inspect communications for commercial reasons. In Opinion 2/2006, adopted on February 2, 2006, the Article 29 Committee clarified that scans by ISPs and ESPs for viruses and spam are lawful interceptions of private communications and justified under both the Data Protection Directive and the e-Privacy Directive, subject to certain limitations. However, the Article 29 Committee also stated that screening for predetermined content and the use of “Did they read it?” programs are almost never permitted under EU law.

Virus Scanning

As viruses can shut down an ISP or ESP’s services and damage the end user’s computer, virus scanning is justified under Article 4 of the e-Privacy Directive, which requires ISPs and ESPs to take “appropriate technical and organizational measures to safeguard security of [their] services.” Moreover, virus scanning is also justified under Article 7b of the Data Protection Directive as such scanning is “necessary for the performance of a contract to which the data subject is a party . . . .” However, ISPs and ESPs must ensure that the content of emails and attachments are kept confidential at all times. If anti-virus and anti-spam programs are designed to scan the content of an email, the contents of the message or attachment can only be analyzed for that purpose.


17 The European Convention on Human Rights authorizes member states to carry out a lawful interception under three conditions, as laid out in Article 8(2): that there is a “legal basis, the need for such a measure in a democratic society, and conformity with one of the legitimate aims listed in the Convention.” An interception is defined as when “a third party acquiring access to the content and/or traffic data related to private communications between two or more correspondents, including traffic data concerning the use of electronic communication services that constitutes a violation of an individual’s right to privacy and to confidentiality of correspondence.”


Spam Filtering

Like virus scanning anti-spam scanning is permitted under Article 7b of the Data Protection Directive as not preventing the proliferation of spam could slow down networks and prevent ISPs and ESPs from providing the services for which they have been contracted. Moreover, because the security of ISPs or ESPs may become a problem insofar as spam affects service, the use of anti-spam filters and the blocking of emails sent from certain addresses is further justified under Article 4 of the e-Privacy Directive. Since blocking email addresses can impact the free transfer of information the Article 29 Committee recommends that ISPs and ESPs allow a user to: (1) opt out of the spam filter; (2) decide what kind of spam to filter out; (3) opt back into spam scanning later on; and (4) read those messages labeled as spam.

Scanning for Predetermined Content

The Article 29 Committee makes clear that ISPs and ESPs are not generally permitted to scan electronic communication for predetermined content, as Article 5(1) of the e-Privacy Directive prohibits “all listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data without the consent of the user concerned,” unless such actions are an “appropriate and proportionate measure” to safeguard national security . . . .” While EU Member States cannot endorse ISPs and ESPs to generally monitor communications in such a way, the Article 29 Committee notes that ISPs and ESPs may offer content scanning as a “value added” service for their subscribers.

“Did They Read It?” Software

The Article 29 Committee expressed its “strongest opposition” to the use of “Did they read it?” processing software, which secretly tracks if an email recipient has read an email, when and how many times it was read, if and to which email server it has been transferred, and what type of web browser was used to open the email. Without the unambiguous consent of the email recipient, such a program is contradictory to the Data Protection Directive and is not permitted.

Duty to Inform

Under the Data Protection Directive, an ISP or ESP also has a duty to inform a subscriber of its virus, spam, and other information processing policies, but the Article 29 Committee determines that such notification can be adequately contained in the contractual conditions of service. Providers of publicly available electronic communication services and networks must also inform subscribers of any particular risks or breaches to network security and what the subscriber can do to fix a breach if the service provider cannot. Also, while actively working to ensure the privacy of personal communication and data, ISPs and ESPs must take positive measures to ensure privacy rights can be exercised.

---

21 e-Privacy Directive, 2002 O.J. (L 201) 37. Article 15(1) allows for member state to restrict the scope of the rights provided for in Article 5 if such a restriction is “a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system.”
SOX Whistleblower Schemes

On February 1, 2006, the Article 29 Committee issued Opinion 1/2006\textsuperscript{23} to provide general guidelines on how companies can comply with both the whistleblower requirements of SOX and EU data privacy law.\textsuperscript{24} The opinion is strictly limited to whistleblower schemes involving accounting, internal accounting controls, auditing matters, fights against bribery, banking and financial crime, and is not a final opinion on whistleblower schemes in general. Whistleblower requirements already exist in most EU states as regards banking and combating bribery, and many states have national laws which mirror SOX provisions. However, the legal obligation laid down by a foreign government (e.g., SOX) does not itself create the legal justification required under the Data Protection Directive to authorize the collection and storage of personal data.

Under EU law, whistleblower schemes are only legitimately established if their purpose is in compliance with either Articles 7(c) or 7(f) of the Data Protection Directive. Article 7(c) authorizes data collection and processing if it is necessary to comply with a legal obligation to which the data controller is subject. Article 7(f) allows for the establishment of a whistleblower scheme if necessary for the purposes of a “legitimate interest pursued by the controller” or by the third party to whom the data is disclosed. Companies that wish to establish whistleblower schemes should obtain a detailed legal analysis, complemented by checks with local data protection authorities to ensure compliance with all local data protection laws that may be more detailed than the Article 29 Committee’s guidelines.

While not a final set of rules, the Article 29 Committee provides a number of suggestions on how to make whistleblower schemes compliant with EU law:

- There should be limitations on who can file a whistleblower complaint and who can be reported as having committed a violation.
- The scheme should emphasize confidential, as opposed to anonymous, reporting by accusers. Anonymous reports can be allowed if the whistleblower scheme does not encourage them and if it is broadcast that an accuser’s identity will be kept confidential unless required for investigative or judicial purposes.
- Data collected must be limited to the purpose of the investigation, and companies must limit the information gathered to accounting, internal accounting controls, anti-bribery, auditing matters, or banking or financial crime issues.
- Any information gathered that is not covered by the whistleblower scheme can be forwarded to the proper officials of the company when the “vital interests of the data subject or moral integrity of employees” are at stake, or when required under national law.

\textsuperscript{23} Article 29 Data Protection Working Party Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime (WP 117), February 1, 2006.

\textsuperscript{24} The status of the law, as SOX applies to European subsidiaries of US companies or European companies listed on US stock exchanges is unsettled, however, as the 1st Circuit US Court of Appeals held that SOX provisions on the protection of whistleblowers do not apply to foreign citizens working outside the US for foreign subsidiaries of companies required to comply with the remaining provisions of SOX.
• All parties that receive the report must provide the same guarantees of security as required of the local EU company under EU law.\footnote{This compliance can be established by a US company’s membership in the US Safe Harbor program, the use of standard contractual clauses, or through the development of corporate data privacy rules that have been pre-approved by the relevant data protection authorities. For more information on Standard Contractual Clauses, see \url{http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf}.}

• All data collected must be promptly deleted, usually within two months of the completion of the investigation, though such data should be kept for the duration of any criminal or other judicial proceedings that may result, including appeals.

• The accused must be notified that data collection has been completed on him, though if notifying the accused might result in the destruction or alteration of evidence such notification can be delayed.\footnote{Article 11 of the Data Protection Directive, 1995 O.J. (L 281). The Working Party did not set a time limit of how long a delay was permissible under such a scenario.}

• The notification must inform the accused of which entity is responsible for the whistleblower scheme, the facts he is accused of, all departments or services that might receive the report, and how to exercise his rights to access and rectify any mistakes in the report.

• The identity of the accuser should remain confidential unless the initial report is found to be malicious, in which case the accuser’s identity can be revealed so that libel proceedings may proceed.\footnote{Article 12 of Data Protection Directive, 1995 O.J. (L 281).}

Passenger Name Record (PNR) Sharing With the US

On May 30, 2006, the European Court of Justice (the “Court”) struck down European Council Decision 2004/496/EC\footnote{Council Decision 2004/496/EC, on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 2004 O.J. (L 183).} (the “PNR Decision”), created to share data on trans-Atlantic airline passengers with the US Bureau of Customs and Border Protection in an effort to prevent terrorism.\footnote{Joined Cases C-317/04 and C-318/04, European Parliament v. Council of the European Union and v. Commission of the European Union, see \url{http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/judgement_ecj_30_05_06_pnr_en.pdf}.} As the data transfer and processing in question fell outside the scope of the Data Protection Directive, the Court determined that the PNR Decision had no legal basis. In the wake of the ruling, the Article 29 Committee adopted Opinion 5/2006 on June 14, 2006, calling for a new EU-wide agreement to be adopted before the now annulled PNR Decision runs out on September 30, 2006, and incorporating the following suggestions:

• Strict limits to the onward transfer of PNR data elements.\footnote{“Data elements” are the fields of information in an airline’s PNR system, of which 34 are currently being transferred, including name, reservation date, travel agent, itinerary, form of payment, flight number, and seating information. See \url{http://www.usembassy.org.uk/terror67.htm}. According to the EU, the US Bureau of Customs and Border Protection has undertaken to continue not to use any PNR data that is defined as “sensitive” in article 8.1 of the Data Protection Directive, including information on race, religion, or health status. See \url{http://ec.europa.eu/comm/external_relations/us/intro/pnrmem03_53.htm}.}

• Reductions in the number of data elements transferred.
• Institution of a “push system,” whereby airlines send the US government PNR data, rather than the US government maintaining its access to, and ability to extract data directly from, airline reservation databases.

• Maintain at least the current levels of data protection.

• Last no longer than the end of November 2007, with regular reviews.

On June 19, 2006, the Commission also passed two initiatives to help move the EU toward creating a new PNR data transfer agreement. Of significance is the Commission’s suggestion that the new agreement be created under Article 38 of Title VI of the Treaty of the European Union, which allows EU Member States to create and adopt the agreement without the involvement of the European Parliament. This is a politically sensitive move, as it was the European Parliament which challenged the original PNR Decision in the courts. Also, as the Court did not find it necessary to address the PNR Decision’s content in order to annul it, the Commission suggests using essentially the same language and legal safeguards as contained in the original PNR Decision. However, unless EU Member States incorporate the European Parliament’s data security and policy concerns, such as through those measures outlined in the Article 29 Committee’s Opinion, it is likely that the European Parliament will again challenge the new agreement in the courts and delay resolution of the issue.

Implications

The recent Commission and Article 29 Committee opinions make clear that more requirements on the handling and transfer of personal data across borders will be forthcoming. In light of the growing pressure for greater regulation, US firms may wish to consider whether they need to review and update their data protection practices for any data transferred to or from the EU. Fresh consideration of participation in the US-EU Safe Harbor program or binding corporate rules may be appropriate as alternatives to model contracts or ad hoc clauses. At the very least, all companies should ensure that contractual clauses used are specifically tailored enough to the transfer to avoid allegations of non-compliance. Moreover, companies involved transferring data from the EU or approved data recipients in third countries may want to begin requiring stricter data security measures from any third party data controllers or processors they utilize, to ease integration with new security requirements that are all but certain to be passed.

While companies involved in internet and email service provision are now assured that anti-virus and anti-spam scanning are legally justified, they must ensure that they do not scan emails and attachments for predetermined content or allow for “Did they read it?” software unless the users provide unambiguous consent. Also, companies that provide publicly available electronic communication services or networks must ensure that all data retained for law enforcement purposes is stored separately from normal business data, and is only processed by select law enforcement agents under strictly controlled conditions.

For companies listed on US stock exchanges, compliance with SOX and EU data privacy law is possible though the law is unsettled in both the US and EU. Until more clarifications are announced, companies should obtain careful analysis of both EU and local law, supplemented by consultations with relevant Data Protection Authorities, to tailor their particular needs in

order to maintain compliance with both the opportunities created by the SOX whistleblower rules and the current limitations of the EU’s application of the Data Protection Directive to the whistleblower element of SOX.

Finally, as regards transfers of PNR data from European airlines to the US government, it is all but certain that a new agreement will be created shortly. However, given the political context, unless the Commission and EU Member States modify the original PNR Decision text to address the European Parliament’s concerns over data security and the US government’s access to airline databases, it is likely that the European Parliament will challenge the new agreement in the courts and further delay any final decision.
This Legislative & Public Policy Advisory is published by Alston & Bird (www.alston.com) to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. The material may also be considered advertising under the applicable court rules. If you have any questions or would like additional information please contact your Alston & Bird attorney or any of the following:

Thomas M. Boyd  
202-756-3372  
tom.boyd@alston.com

Paul G. Martino  
202-756-3439  
paul.martino@alston.com

Thomas E. Crocker  
202-756-3318  
thomas.crocker@alston.com

Robert C. Reynolds, Jr.  
202-756-3368  
bob.reynolds@alston.com

David C. Keating  
404-881-7355  
david.keating@alston.com

Dwight C. Smith, Ill  
202-756-3325  
dwight.smith@alston.com

Yukiko Ko  
202-756-3311  
yukiko.ko@alston.com

Jonathan M. Winer  
202-756-3342  
jonathan.winer@alston.com

Kathryn Marks  
202-756-3479  
kathryn.marks@alston.com

© Alston & Bird LLP 2006