ALSTON&BIRD

WWW.ALSTON.COM

GKH LAW OFFICES GROSS ▪ KLEINHENDLER ▪ HODAK HALEVY ▪ GREENBERG & CO.

Privacy & Security ADVISORY ▪

DECEMBER 8, 2015

It's Not Just Europe: Why 2016 Cloud Vendor Management Programs Should Address Evolving Global Privacy and Cybersecurity Risks

By Dominique R. Shelton, Teri McMahon, David Caplan and Evan Sippel-Feldman of Alston & Bird, and Heather Stone, Sigal Lewkowicz and Ella Tevet of Gross, Kleinhendler, Hodak, Halevy, Greenberg & Co.

Introduction

2015 has seen landmark changes in privacy and cybersecurity laws and regulatory best practices. These developments have had a direct impact on cloud vendors. For example, evolving judicial and regulatory interpretations of pre-existing cross-border transfer laws are transforming the ways that personal data can be managed in the cloud. Also, this year, U.S. regulators have issued *four* written guidance reports calling for companies to monitor the data security practices of their vendors.[i] These written guides signal heightened regulatory attention to the issue of vendor security going forward. This may force vendors to revisit pre-existing contractual terms that often place privacy and data security legal compliance exclusively on cloud customers.

Also, cloud vendors will find their operations increasingly impacted by privacy and data security developments based upon the sheer volume of personal data at issue. Almost overnight, companies have collectively migrated thousands of terabytes of data en masse from their own servers to cloud vendor environments.[ii] Cloud vendors offer simplified solutions to companies for essential business functions such as customer relations management (CRM),[iii] human relations/employee benefits[iv] and data management platforms (DMPs),[v] to help target the purchase and sale of online advertising. Some household names in the cloud-based service provider industry emanate from Silicon Valley (e.g., Salesforce, Workday and Oracle). Perhaps lesser known—but increasingly impactful—is the number of sizable cloud-related vendors originally emanating from Israel and purchased by U.S. companies (e.g., SAP enterprise software, Visual Tao and CTERA Networks).[vi] With developments like Google's recent purchase of the Israeli-founded Waze app[vii]

for a reported $1 billion and Microsoft's recent purchase of Israeli-founded cloud security firm Adallom,[viii] some have argued that the Israeli tech community is second in line globally only to Silicon Valley. [ix]

Cloud environments and other technology vendors that rely on cloud storage (e.g., mobile app developers) have simplified the lives of many marketing, HR and tech professionals in small businesses to the Fortune 500 alike. Nevertheless, cloud vendors and their customers should pay heed to legal requirements and best practices impacting privacy, as well as security, going forward. Accordingly, now is the time for cloud vendors and the companies that hire them to revise or develop new policies and procedures to ensure that vendors are properly managing data collection, transfer and storage of personal information. Failure to do so could create substantial liabilities for cloud vendors and the customers they serve.

This advisory highlights some of the top new privacy and cybersecurity developments that impact cloud vendor relationships in the U.S., EU, Israel, Dubai and beyond.

I. Privacy Developments That Impact Cloud Vendors.

Recent developments in the EU/European Economic Area (EEA), Dubai, Israel and the U.S. discussed below, have significantly changed the landscape such that these new privacy concerns should become key components of vendor management programs in 2016 for cloud computing companies.

A. Global Cross-Border Transfer Developments

1. EEA Privacy Cross-Border Transfer Developments

Under EU law, the U.S. does not have "adequate protection" for personal data. Accordingly, up until October 6, 2015, the EU permitted personal data to be transferred to the U.S. under four circumstances, most germane to cloud vendors: (1) Safe Harbor; (2) binding corporate rules (BCRs); (3) standard contract clauses (also known as "model contracts"); and (4) consent.[x] While other mechanisms for cross-border transfer *technically* exist under EU law (i.e., permits, derogations and bilateral agreements to enhance law enforcement), either EU data protection authorities have roundly rejected them as unsuitable for the types of mass transfers of consumer and HR data at the core of many commercial cloud contracts or they are otherwise largely inapplicable.[xi] Accordingly, several U.S.-based cloud vendors relied on the Safe Harbor program to support transfers of personal data from the EU to the U.S. until recently.[xii] On October 6, 2015, in the landmark decision *Maximillian Schrems v. Data Protection Commissioner*, the European Court of Justice (ECJ) ruled the Safe Harbor framework invalid and transfers made to the U.S. under it illegal.

In the aftermath of *Schrems*, EU regulators have made it clear that the decision will not be challenged. To the contrary, on October 16, 2015, while still expressing hope for a new iteration of Safe Harbor, the Article 29 Data Protection Working Party confirmed its alignment with the ECJ's decision on the pre-existing version and signaled enforcement would commence by late January 2016 if a new agreement is not negotiated.[xiii] Similarly, on October 22, 2015, the Swiss Federal Data Protection and Information Commissioner (FDPIC)[xiv] announced that the U.S.–Swiss Safe Harbor was also invalid. The FDPIC also called for existing data transfer contracts to be amended by the end of January 2016 to include explicit disclosures that U.S. authorities may access personal data if transferred there.[xv]

On October 26, 2015 the independent data protection authorities of the German federal and state governments issued a Safe Harbor update.[xvi] Extending the rationale of *Schrems*, the German DPAs announced they will not issue any new authorizations for data transfers to the U.S. even if based upon BCRs or model contracts. The German DPAs recognized that consent may in certain limited circumstances provide a legal basis for data transfers, but indicated that it is not generally suitable for mass data transfers—like those at issue for many cloud providers. One German DPA issued separate guidance reflecting invalidation of model contracts.[xvii]

In its recent November 6, 2015, guidance (November 6 Commission Guidance), the European Commission confirmed that in light of the *Schrems* decision, it is "clear that data transfers between the EU and the United States can no longer be carried out on that basis…."[xviii] The November 6 Commission Guidance also noted that three cloud providers had already announced alternative tools for cross-border transfers, including model contracts and options for customers to process EEA data in the EEA.[xix]

On November 18, 2015, the Norwegian DPA announced that he "discourages the transfer of personal data based on the consent of the individual alone but rather recommends obtaining his approval prior to conducting any transfers to the U.S."[xx]

All of the developments described above—as well as others that will surely follow—should prompt companies to assess in connection with their cloud vendors (a) whether the company's data includes personal information transported to the U.S. from the EEA and (b) if so, what mechanisms the cloud vendors put in place to ensure lawful transfer. If, on the other hand, a company does not have operations in the EEA, and would not ordinarily have a need to process data there but for the locations of the cloud vendor's data centers, it may question whether executing a model contract would create new obligations under EU law that would not otherwise exist. In turn, cloud vendors should be prepared to research solutions that will protect their customers from facing regulatory enforcement at the end of January 2016 in the EEA.

2. Israeli Privacy Cross-Border Transfer Developments

Also concerning for U.S. companies that rely on Israel's burgeoning tech community for cloud services, was the Israeli Law, Technology and Information Authority's (ILTA) October 19, 2015, decision invalidating transfers from Israel to the United States premised upon the reasoning of *Schrems*.[xxi] Companies working with Israeli vendors should:

- First, review all existing agreements and determine what data protection measures the vendor is obliged to maintain. Be sure that the vendor can meet those measures. Consider whether the existing agreements can be easily terminated if Safe Harbor is invalid and no alternative mechanism is provided in its stead.
- Second, select an alternative method for transferring personal data from Israel to the U.S. The exceptions available under the applicable regulations allow:
    - Data transfer pursuant to an agreement with the database owner under which the transferee

undertakes to comply with applicable Israeli law (organizations that want to base such contractual obligations on the model contract clauses adopted by the European Commission may do so subject to certain necessary modifications); or

- Obtaining the unambiguous consent of the data subject to the transfer.

3. Dubai Cross-border Transfer Developments

Cross-border issues could also affect cloud vendors servicing the financial industry from Dubai. On October 26, 2015, the commissioner of data protection for the Dubai International Financial Centre (DIFC) indicated that data controllers transferring personal data to the U.S. cannot rely on the Safe Harbor scheme post-*Schrems*.[xxii] Instead, they were encouraged to rely on alternative methods for data transfer under the DIFC Data Protection Law (No. 1 of 2007) and related DIFC data protection regulations. The commissioner expressly noted his intention to monitor Safe Harbor 2.0 discussions to glean whether a future protocol may emerge.[xxiii]

Financial institutions in the U.S. that rely upon cloud vendors to transfer personal data from the DIFC should review the basis upon which their cloud vendors transfer personal data from the DIFC to the U.S. to ensure compliance with the current interpretations of the DIFC data protection requirements.

II. Data Security and Cybersecurity Developments

A. U.S. Regulatory Guidance and Enforcement

Throughout 2015, U.S. regulators have issued pointed guidance regarding cybersecurity best practices for vendor management. Recommended practices include calls for companies hiring vendors to (1) conduct pre-contract due diligence that incorporates a risk assessment[xxiv] and (2) include security standards for vendors in the contract, such as encryption requirements.[xxv] These particular recommendations have been followed by industry for years. That said, regulators have crafted additional recommendations based on *new* enforcement actions announced within the past 16 months.[xxvi]

Therefore, companies should not assume they already know the contents of new regulatory guidance issued in 2015 without first reading the guidance closely. The simple fact that *regulators* (as distinct from industry players) have issued written guidance this year reflects regulator resolve to scrutinize vendor management more closely.

Accordingly, companies should consider comparing their existing practices with 2015 regulator guidance to see how they align or differ. Ignoring regulatory guidance, on the assumption that it is already known, could place companies at greater risk of facing regulatory enforcement actions.[xxvii]

B. Israeli Data Security Laws & Enforcement

The Israeli Privacy Law imposes obligations on the owners, "holders" and "managers" of databases and on the use of data held in such databases. The law stipulates that the owner, holder and manager, severally, are responsible for the information security of the data processed in the database. In addition, specific privacy protection regulations[xxviii] require the database manager to appoint an information security manager and

establish the responsibility of database managers for the information security of the data processed in the databases.

Like the U.S. and EEA, heightened security recommendations exist in Israel for health and financial data. For example, starting January 1, 2016, health institutions will be required to only contract with suppliers that are ISO 27001 or ISO 27799 compliant. On March 16, 2015, the supervisor of banks at the Bank of Israel, issued a directive regarding cyber defense management. The directive requires banking corporations to place special emphasis on cyber defense and take the necessary steps to effectively manage cyber-related risks. The directive lays out the principles according to which banking corporations are required to operate in the area of cyber defense. The directive went into effect on September 1, 2015.

Companies doing business in Israel, whether in their capacity as vendors or by contracting with Israeli vendors will want to ensure compliance with this new body of law in their vendor agreements.

III. Corporate Due Diligence

New cloud vendors, like other startups, are often looking for an exit strategy that involves a large liquidity event where they are either purchased as part of a merger and acquisition transaction or go public. Given the current risk profile, privacy and cyber due diligence should become part of every due diligence effort involving cloud/tech vendors. Failure to do so may haunt investors later.

IV. Conclusion

In today's highly dynamic environment, companies have a heightened need to pay attention to privacy and cybersecurity issues, particularly regarding their cloud vendors. Regulator guidance indicates that companies are expected to consider privacy and security in their vendor management programs—and this includes clouds. If this has not already been done, attention to this area should be a priority for 2016 planning.

I. Four reports were issued in February, March, April and June 2015, respectively: (1) The Financial Industry Regulatory Authority, Report on Cybersecurity Practices (Feb. 2015) ("FINRA Report"), at 26 (for section titled "*Vendor Management*") *available at* https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf; (2) The Communications Security, Reliability and Interoperability Council IV, Working Group 4, Final Report Small and Medium Business Cybersecurity Risk Management and Best Practices (Mar. 2015) ("CSIRC IV WG4 Report") at 10, 26 and 59, *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf; (3) *Enhancing Cybersecurity of Third-Party Contractors and Vendors,* Before *the House of Representatives, Committee on Oversight and Government Reform*, Apr. 22, 2015 ("COGR Hearing"), *available at* https://oversight.house.gov/hearing/enhancing-cybersecurity-third-party-contractors-vendors/; and (4) Federal Trade Commission, Start With Security (June 2015), ("Start With Security") at 11 (section titled "*Make sure your service providers implement reasonable security Measures*") *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

II. Sue Poremba, *Need terabytes of cloud storage? No problem...*, Cloud Tech, (Mar. 14, 2013), *available at* http://www.cloudcomputing-news.net/news/2013/mar/14/need-terabytes-of-cloud-storage-no-problem/.

III. Software as a service (SaaS).

IV. Platform as a service (PaaS).

V. Infrastructure as a service (IaaS).

VI. David Shamah, *Cloud cover: Israel's top eight cloud computing firms*, Israel 21C (Mar. 10, 2011).

VII. The Waze app itself stores data on clouds. Waze Privacy Policy (section titled "Sharing Information With Others"), *available at* https://www.waze.com/legal/privacy (last visited on November 30, 2015).

VIII. Takeshi Numoto, *Microsoft acquires Adallom to advance identity and security in the cloud*, The Official Microsoft Blog, (Sept. 8, 2015), *available at* http://blogs.microsoft.com/blog/2015/09/08/microsoft-acquires-adallom-to-advance-identity-and-security-in-the-cloud/.

IX. Eilon Tirosh, *Israeli cooperation and collaboration is making Silicon Wadi the Valley's major competitor* VentureBeat, (February 25, 2014), *available at* http://venturebeat.com/2014/02/25/the-native-israeli-character-is-making-silicon-wadi-the-valleys-major-competitor/.

X. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive 95/46/EC" or "Data Protection Directive"), Art. 26(1).

XI. *See e.g.*, Article 29 Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114) (Nov. 25, 2005) at 9 ("…the Working Party would recommend that transfers of personal data which might be qualified as repeated, mass or structural should, where possible, and precisely because of these characteristics of importance, be carried out within a specific legal framework (i.e. contracts or binding corporate rules).").

XII. *See*, Safe Harbor list, *available at* https://safeharbor.export.gov/list.aspx (including U.S.-based cloud providers such as Salesforce, Workday, Adobe and Oracle as participants in Safe Harbor).

XIII. Statement of the Article 29 Working Party (10/16/2015), *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

XIV. *Suite De L'arrêt Concernant L'accord «Safe Harbor»: Indications Utiles Pour La Transmission De Données Aux États-Unis* (October 22, 2015), *available at* http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr (translated in French, Spanish and Italian).

XV. *Id*.

XVI. The German DPAs October 26, 2015 position paper is available in German. *See Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)* (Oct. 26, 2015), *available at* https://www.datenschutz.hessen.de/ft-europa.htm#entry4521.

XVII. The DPA of the German state of Schleswig-Holstein issued a separate guidance on October 14, 2015, taking the position that model contracts are no longer valid. *Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14* (Oct. 14, 2015), *available at* https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf (in German).

XVIII. November 6 Commission Guidance at 14.

XIX. November 6 Commission Guidance at 12, n. 40. Other cloud providers are responding to the *Schrems* decisions with offerings in the EEA. Barb Darrow, *Tech Companies are Seizing on the Collapse of the Safe Harbor Agreement*, Fortune Magazine (November 17, 2015), *available at* http://fortune.com/2015/11/17/tech-providers-safe-harbor/.

XX. Adequacy: Norwegian Organisations Must Obtain the Authorisation of the DPA Prior to Conducting Data Transfers to the U.S. (Nov. 18, 2015), *available at* https://www.privaworks.com/Details/AlertReference.aspx?guid=%7b1401050a-9229-4ca0-8cde-404b91cd3b95%7d&mode=fr&u=0feebca0-bead-4ea9-904d-3f90e3ca291f.

XXI. ILITA *Court of Justice of the European Union Invalidates the Safe Harbor Arrangement for Transfer of Personal Data from Europe to the United States* (October 19, 2015), *available at* https://iapp.org/media/pdf/resource_center/ILITA_SH_Statement.pdf.

XXII. Office of the Commissioner of Data Protection, DIFC Data Protection Commissioner Guidance on Adequacy Status Relating to U.S. Safe Harbor Recipients (October 26, 2015), *available at* http://www.difc.ae/sites/default/files/DIFC-Data-Protection-Commissioner-Guidance-on-Adequacy-Status-relating-to-U.S.-Safe-Harbor-Recipients.pdf.

XXIII. *Id*.

XXIV. FINRA Report at 26. *See also*, COGR Hearing.

XXV. Start with Security at 11. See also, FINRA Report at 26 and COGR Hearing (where Mr. Gregory Wilshusen, director of information security issues at the U.S. Government Accountability Office stated, "Encrypting sensitive data is a basic fundamental security control, and I would certainly

recommend that most companies use it to the extent that they have sensitive information that needs protection.").

[xxvi] *In re GMR Transcription Servs., Inc.*, No. 122 3095 (F.T.C. Aug.14, 2014), Docket No. C-4482 (where the FTC enforced against a company for failing to require its vendors to exercise reasonable security).

[xxvii] *Id*.

[xxviii] Takanot Haganat Pratiut (Tnayei Haĥzakat Meyda ve'Shmirato ve'Sidrei Ha'avarat Meyda Bein Gufim Tziburiyim) [Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data between Public Bodies)], 5746-1986, 5740-1980 KT 1480; 5745-1985 KT 1146 (Isr.).

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Security Group

Atlanta

Kacy McCaffrey Brake
kacy.brake@alston.com
404.881.4824

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

Angela T. Burnette
angie.burnette@alston.com
404.881.7665

David Carpenter
david.carpenter@alston.com
404.881.7881

Lisa H. Cassilly
lisa.cassilly@alston.com
404.881.7945

Julia Dempewolf
julia.dempewolf@alston.com
404.881.7169

Maki DePalo
maki.depalo@alston.com
404.881.4280

Clare H. Draper IV
clare.draper@alston.com
404.881.7191

Peter K. Floyd
peter.floyd@alston.com
404.881.4510

James A. Harvey
jim.harvey@alston.com
404.881.7328

John R. Hickman
john.hickman@alston.com
404.881.7885

William H. Jordan
bill.jordan@alston.com
404.881.7850
202.239.3494

David C. Keating
david.keating@alston.com
404.881.7355

W. Scott Kitchens
scott.kitchens@alston.com
404.881.4955

Dawnmarie R. Matlock
dawnmarie.matlock@alston.com
404.881.4253

Teri Lynn McMahon
teri.mcmahon@alston.com
404.881.7266

Bruce Sarkisian
bruce.sarkisian@alston.com
404.881.4935

Peter Swire
peter.swire@alston.com
404.881.4259

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael R. Young
michael.young@alston.com
404.881.4288

Los Angeles

David Caplan
david.caplan@alston.com
213.576.2610

Kimberly K. Chemerinsky
kim.chemerinsky@alston.com
213.576.1079

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

Katherine E. Hertel
kate.hertel@alston.com
213.576.2600

Sheila A. Shah
sheila.shah@alston.com
213.576.2510

Dominique R. Shelton
dominique.shelton@alston.com
213.576.1170

Evan Sippel-Feldman
evan.sippel-feldman@alston.com
213.576.1098

Washington, D.C.

Louis S. Dennig IV
lou.dennig@alston.com
202.239.3215

Kimberly K. Peretti
kimberly.peretti@alston.com
202.239.3720

Eric A. Shimp
eric.shimp@alston.com
202.239.3409

Paula M. Stannard
paula.stannard@alston.com
202.239.3626

Jason R. Wool
jason.wool@alston.com
202.239.3809

If you would like to receive future *GKH IP Advisories* electronically, please forward your contact information to **gkhpublic@gkh-law.com**. Be sure to put **"subscribe"** in the subject line.

If you have any questions or would like additional information, please contact your GKH attorney or one of the following:

GKH LAW OFFICES — GROSS ▪ KLEINHENDLER ▪ HODAK HALEVY ▪ GREENBERG & CO.

Heather A. Stone
+972-3-607-4520
heather@gkh-law.com

Ella Tevet
+972-3-607-4541
ellat@gkh-law.com

One Azrieli Center, Round Building | Tel Aviv 6701101, Israel | Website: www.gkhlaw.com

ALSTON & BIRD

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com