Data privacy considerations in telecommunications M&A: do you know your risk?
Data privacy considerations in telecommunications M&A

Global M&A activity among telecommunications (telco) companies reflects the ongoing transformation impacting the sector in response to increasing competitive intensity, evolving consumer behaviors and disruption from so-called “over-the-top” (OTT) players, which deliver audio, video or other media over the internet without the involvement of a multiple-system operator in the control or distribution of the content.

Within this context, M&A transactions (whether buyer or seller focused) among telco companies, irrespective of where the transaction occurs or what countries are impacted, will likely be subject to data privacy laws, requirements and obligations.

Efforts to update regulations regarding privacy and personal data protection are underway in several countries and regions, most notably the European Union (EU), which has introduced the General Data Protection Regulation (GDPR) package (further discussed below).

Compliance requirements for operators are in flux, particularly as regulators seek to strike a balance between consumer protection and national security needs. In this light, keeping pace with the different policy initiatives at a national and international level is more important than ever for operators.

In addition, telco companies face critical challenges around existing contracts with customers and third parties for the storage and delivery of information that in many cases may not be in accordance with the new EU legislation. In such cases, telco companies will need to closely examine the details and challenges within existing contractual arrangements (e.g., location of, and access to, the data) to further determine the degree of potential exposure and measures that may be required to mitigate a potential breach of the legislation.

EU General Data Protection Regulation

The EU, as the unofficial global leader in data privacy protection, recently approved the General Data Protection Regulation, which will generally impose stricter data privacy controls with respect to the personal data of EU citizens, effective May 2018. In general, the GDPR covers the following areas:

- Penalties for breach of the new data protection rules: possible fine of up to the greater of €20 million or 4% of the global annual turnover
- Principle of accountability: policies and procedures
- Information technology (IT) and cybersecurity
- Privacy impact assessments
- Privacy by design and default

- Mandatory data breach notification
- Specifics on big data and profiling
- Restrictions and requirements on exporting data outside Europe
- Right to be forgotten and erasure of data

The GDPR will have far wider coverage than current EU data privacy law and, once it becomes effective in May 2018, will result in even fewer, if any, data privacy “free zones” remaining in the world.

Legal interception and data retention regulation

Legal interception (LI) and data retention (DR) are usually highly regulated in most countries. Mandatory processes and technical measures should be in place in order to deal with court warrants and law enforcement agency directives. Failure to be in compliance with the legal requirements could result in, depending on the country, significant fines; even the operator license could be at risk. In an M&A context, the buyer should be confident that the acquired company is free of risk with regard to the LI and DR topics. On the other hand, a telco operator that is not highly scrupulous in managing the secrecy of its own clients’ communications could face reputational damage due to improper management of the interception functionalities of their networks.

NIS directive

The Directive on Security of Network and Information Systems (NIS Directive) is closely linked to privacy regulation, especially around security incident management and coordination. Although the directive is still to be transposed into the national laws, telecommunication services will be identified as essential services and therefore under the scope of the directive.

Introduction to data privacy in telco sector M&A transactions

Most M&A transactions in the telco sector require parties to exchange at least some personally identifiable information or personal information (PI), whether it is the seller’s employees’ PI or its customers’ PI, and privacy/data protection and information security (data privacy) are now global issues regulated in most countries.

Addressing data privacy compliance is therefore important for most telco sector M&A transactions in most countries impacted by such transactions. Addressing data privacy at the early stage of an M&A transaction will allow sufficient time for any necessary remedial steps, in terms of both the transactions and the target’s compliance, without unduly delaying the transaction.
While data privacy concerns and compliance are often overlooked (at least until after the transaction has concluded), the new or significantly revamped data privacy environment of most countries will likely be brought into play by the transaction. In addition, the very real prospect of fines for breaches, possible breaches of directors’ duties, class or representative complaints, or legal actions (and the damages and compensation arising from such issues), along with a potential loss of reputation, places greater importance on data privacy compliance in terms of both the (i) transfer and collection of PI as part of the due diligence review or the transaction; and (ii) target’s compliance with the relevant data privacy laws in all relevant countries in which business is conducted.

What data privacy laws are applicable?

Before considering the general data privacy “dos and don'ts” and some country-specific data privacy issues, telco companies should remember that the data privacy laws of most countries usually cover and regulate the collection, use and disclosure of PI. In most jurisdictions, PI is usually defined to include any data or information (whether fact or opinion) relating to an identified or reasonably identifiable individual. The contact information for an individual business contact at a seller’s customer are, for example, often considered PI together with the more obvious information held on individuals generally.

In many jurisdictions, sensitive information is a subset of PI and is defined as PI that relates or refers to an individual's health, sexual orientation or practices, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, social security, tax file or national identity number, criminal record or genetic or biometric information and, occasionally, financial information, including account numbers and passwords (to name a few). In many jurisdictions, sensitive information is treated differently from general PI, often requiring consent to be collected, used or disclosed and attracting a higher level of obligations (e.g., around securing the information).

The collection and use of PI in most countries requires at least prior notice of (if not consent to) certain mandatory matters and, for sensitive information, often requires the unambiguous and informed prior consent of the relevant individual to the proposed collection, use or disclosure of such information (if allowed at all).

In addition, the transfer of PI outside of the relevant local country often requires that certain obligations must first be met by the transferee, and in many cases, the transferee will continue to have some responsibility (if not liability) for the PI it sends outside that country, including for the actions of the offshore recipient that, if conducted onshore by the transferee company, would have been a breach of that country’s data privacy laws.

Generally applicable privacy dos and don'ts relevant to the collection, use or disclosure of PI in telco M&A transactions

The shifting compliance burdens regarding data protection and retention require that operators have clear viewpoints on their roles as custodians of customer data.

In that regard, any party in a telecommunications M&A transaction obtaining or using PI (even if provided as part of due diligence) should:

- Designate a person (or team) that is responsible for data privacy issues/compliance
- Limit collection/disclosure of PI to a minimum and to that actually required for the transaction
- Limit internal and external distribution of PI on a “need-to-know” basis
- Use only secure methods to share PI (e.g., use of the basic version of Dropbox, with limited security and inability to track forwarding of information, will not be appropriate)
- Be particularly careful with sensitive information, including ascertaining the right to use it for the purposes required and to disclose it to a potential purchaser in the transaction
- Confirm awareness of when it is required to give notice to or obtain consent from those individuals whose PI is being disclosed or collected
- Verify that PI is deleted or de-identified when it is no longer needed for the notified purposes
- Contractually oblige the recipient to comply with the relevant data privacy laws and limit their use of the PI solely to the purposes of the due diligence review, for example

At all stages of the transaction, from the initial contact or the memorandum of understanding to the completion of the transaction, data privacy issues need to be addressed by both the buyer and seller. In particular, although often overlooked, the receipt of PI by a potential buyer from the seller as part of the due diligence process is often considered by data privacy law to be a collection of PI by that potential buyer, and therefore the buyer must comply with all relevant data privacy laws.

The potential buyer, on receipt of PI from the seller (or other third party), will often have its own data privacy obligations with respect to notice and the holding and use of such PI under the applicable local data privacy laws. Also, should a potential buyer not proceed with the transaction, most data privacy laws impose an obligation on that potential buyer to de-identify or destroy such PI as soon as practicable.
For telco sellers

Just as in other areas of its business requiring compliance, the seller in the transaction should confirm that it is compliant, from a data privacy perspective, in order to enable a smooth transaction. This includes verifying that all relevant data privacy policies and processes are in place and that:

- Any prior data privacy notice or purposes disclosed to individuals cover the intended disclosure to the potential buyer as part of due diligence
- Appropriate technical and organizational security measures are in place to prevent unauthorized, unlawful or accidental loss, destruction of or damage to the PI
- If the PI is to be disclosed outside the country where it was collected or is currently held, the appropriate purposes and disclosure (to allow overseas disclosure) have been consented to in the relevant documentation prior to or at the time of the original collection of the PI
- For sensitive information, the seller has each relevant individual’s consent to disclose that information for the purposes of the due diligence or overseas, as the case may be
- The seller’s existing privacy policy or notice originally provided on the collection of the PI does (or can be construed to) cover the disclosure of PI to a potential buyer as part of due diligence or the transaction

In most cases, it is going to be impractical or inappropriate at the time of the transaction to provide relevant notice or gain relevant consents for the due diligence disclosure (especially if the transaction is market sensitive or to be kept secret).

Even if a sale is not currently being contemplated, sellers should review data privacy policies to see if disclosure of PI in a contemplated transaction due diligence scenario has been identified as a purpose or potential disclosure in their existing privacy policy/notice. If not, such policies should be amended as a leading practice.
For telco buyers

It is important that buyers not only consider the seller's general compliance with all relevant local data privacy laws (or any other relevant country’s data privacy laws) in the conduct of the seller’s business, but also consider their own data privacy obligations in respect of their receipt (i.e., collection), use and disclosure of any PI provided to them by the seller as part of the due diligence process. With regard to the collection of PI as part of the due diligence process, buyers should consider:

- What obligations they have in respect of notification of collection
- If sensitive information is collected, what obligations there are with respect to obtaining consent
- What warranties or guarantees are provided by the seller that it is able to provide such PI or sensitive information to (and for what purposes such PI or information can be used by) the potential buyer (and make certain these are included in the nondisclosure agreement or sale agreement)
- What obligations (both at law and pursuant to the nondisclosure agreement) apply to the potential buyer if the transaction does not proceed
- What obligations (both at law and under the sale agreement) apply if the transaction does proceed

In addition, when considering the compliance health of the seller, the buyer needs to also consider:

- Identifying the type of PI collected, used and disclosed by the seller in its business
- Identifying whether appropriate notification has been given or consent obtained (this includes both the consideration of the relevant data privacy policy setting out the purposes for collection as well as the processes; that is, when and how such notification or consent was delivered or obtained in the collection process)
- Identifying any compliance failures or areas of compliance concern and, if possible, getting them remedied before completion
- Ascertaining what areas of compliance concern need to be warranted or indemnified by the seller
- Setting up a plan of action for post-completion actions to fix any identified data privacy compliance concerns

Generally applicable privacy dos for all buyers in a transaction (in addition to those mentioned above) include the following. Do:

- Identify PI to be retained and to be transferred as part of the process
- Implement appropriate technical and organizational security measures in respect of the transaction processes (e.g., information provided as part of the due diligence needs to be kept separate and destroyed/returned if the deal does not proceed)
- Assess the target’s data privacy compliance
- Confirm the ability of the target to lawfully use the relevant PI and, if relevant, its ability to disclose or sell such information
- Identify data privacy risks and either fix or reduce them or allocate liability for them in the sale and purchase documentation

In addition to those mentioned above, some of the generally applicable don’ts for buyers in an M&A transaction (no matter where such transaction occurs) include the following. Don’t:

- Start the transaction process without having considered the data privacy implications
- Assume the target’s compliance; you must perform your own due diligence on this
- Wait until the last minute to consider data privacy compliance
- Forget (or choose not) to implement relevant information security measures in respect of the transaction processes
- Assume that the seller will provide all necessary information
- Ignore or underestimate the data privacy issues identified and their potential impact
- Collect, retain or process as part of the due diligence process more PI than is absolutely necessary for your legitimate purposes and the due diligence
- Underestimate or ignore any post-acquisition steps (or fail to implement such steps) required to achieve appropriate data privacy compliance

Conclusion

The data privacy issues noted above relating to telco M&A transactions are not insurmountable. They will be uncovered through appropriate consideration and due diligence and are often dealt with via pre- or post-transaction remedial action or allocation of risk through the agreement, or both. However, it is clear that data privacy, both in terms of the transaction processes (in particular, the due diligence review) as well as the target's business compliance, is now a key consideration in all telco M&A transactions.
Specific country telco M&A transaction data privacy issues

Below, we briefly note the specific requirements, issues and dos and don’ts for a number of specified countries, which are in addition to or different from those noted above as generally applicable to data privacy in most telco sector M&A transactions, no matter where they occur and the countries that are impacted.

Australia
The two additional Australia-specific data privacy issues to be considered in any M&A transaction involving or relating to Australia are:

- Telecommunications data retention obligations
- Mandatory data breach notification

Data retention
The data retention regime, effective from 13 October 2015, applies to all carriers, carriage service providers and internet service providers who own or operate any telco infrastructure in Australia and requires the keeping of metadata relating to or associated with communications via email, mobile phones and landlines.

The resulting additional data privacy issues potentially impacting relevant telco M&A transactions related to Australia are:

- Has the target complied with its data retention obligations to date, and if not, what will it cost to do so?
- Does the buyer, if not an Australian entity, understand the full scope of what will be continuing, complex and onerous data retention obligations after acquisition?
- Has the target complied with increased data privacy obligations in respect of the retained data (which is all deemed to be PI)?

Mandatory data breach notification
Mandatory data breach notification is law and will become effective in Australia on 22 February 2018; this will significantly increase:

- Data privacy obligations and compliance requirements in Australia
- The costs associated with (and the public awareness of) data breaches

Thus, while the law is generally applicable across all businesses, any Australia-related telco M&A transaction will also be impacted. The potential relevant issues are:

- Is the target (if Australian) ready for mandatory data breach notification, and if not, how much will it cost to get them ready?
- Will the buyer’s other businesses or data (even if outside Australia) be impacted by, or become subject to, Australian data mandatory breach notification (e.g., by mingling of Australian PI) after the acquisition?

France
French privacy rules for telco providers derive from the ePrivacy Directive 2002/58/EC but also contain specific provisions regarding mainly data retention of information related to communications.

a. Secrecy of correspondence
Under Article L33-1 of the Postal and Electronic Communications Code (Code des postes et des communications électroniques, or CPCE), all “transmitted messages and information related to communications,” whether circulated by post or by telecommunication means, are subject to the “secrecy of correspondence.” In France, the violation of the secrecy of correspondence is currently punished by Articles 226-15 and 432-9 of the French Criminal Code with one to three years of imprisonment and a fine of €45,000.

b. Data retention: principle of deletion or anonymization
According to Article L34-1 of the CPCE, traffic-related data shall be deleted or anonymized.

However, the following exceptions are provided under the same article:

i. The telco provider has the right to retain certain data for invoices and security purposes (Art. L34-1 IV).

Regarding invoicing purposes, the data (e.g., user identifying information, data related to the equipment used, technical data as well as the date, time and duration of each call and data on additional services) may be retained until the end of the deadline for legal proceedings against the invoice and shall not exceed one year.

Regarding security purposes, the allowed retention period is up to three months.

ii. The data operator has the obligation to retain for judicial or administrative requisition.

French law provides an obligation to retain traffic data for one year in order to respond to a judicial or administrative requisition for the purposes of investigation, establishment and prosecution of criminal acts (Article L34-1-III of the CPCE). This data must include, according to Article R10-13 of the CPCE, the following information: user identifying information; data related to the equipment used; technical data as well as the date, time and duration of each call; data on additional services requested or used and their suppliers; data identifying the intended recipient of the communication; data identifying the origin of a call and the location of the communication.
The CPCE also provides for the retention and processing of traffic data for purposes of commercializing telco or value-added services but only under the express consent of the data subject. Consent is also required for processing data, making it possible to locate the terminal equipment of the user for purposes other than the routing of the relevant communication.

Finally, telco providers are subject to the obligation to notify the French Data Protection Authority of any data breaches.

**Forecast for the proposed European ePrivacy Regulation**
The overview provided below with respect to Germany regarding the impact and the upcoming changes of the new telco-related privacy framework also applies for France, as a regulation applies to all Member States without providing national legislators with powers to adapt the rules.

** Please note that the above brief overview of data privacy rules for telco providers in France does not cover data privacy provisions not related to the telco industry, such as data protection rules enacted under the French Data Protection Act, which transposes Directive 95/46/EC and the non-sectorial privacy rules provided by Directive 2002/58/EC as transposed in local law either in the French Data Protection Act or in the Postal and Electronic Communications Code.

**Germany**

Under the current law in Germany, telco providers are subject to the sector-specific data protection and IT security rules set out in Sections 88-115 of the federal Telecommunications Act (Telekommunikationsgesetz, or TKG); these rules are mainly based on the provisions of European ePrivacy Directive 2002/58/EC, but also contain some non-EU-based provisions, e.g., the provisions concerning data retention.

Content and metadata of telecommunications fall within the scope of telecommunications secrecy (Section 88 TKG) and therefore enjoy special protection.

Without the consent of the concerned data subject(s), telecommunications metadata may in principle only be processed for the purposes set out in Section 96 ff. TKG, e.g., for the purpose and to the extent necessary to establish and maintain a telco connection or for billing purposes. Metadata that is not necessary for these purposes (e.g., metadata of customers with flat rates) shall in principle be deleted after termination of the telco connection.

There are two main exceptions to that principle:

- Telecommunications metadata may be stored for up to seven days to detect, locate and eliminate faults and malfunctions in telco systems and for abuse handling (e.g., distributed denial-of-service attacks).
- Furthermore, there is a data retention obligation for a period of four respective 10-week periods concerning telco metadata (e.g., time, internet provider addresses, location data, cell IDs, phone numbers) for the purposes of public security or prosecution of serious crimes.

Section 109 ff. TKG also contains special provisions concerning technical security measures as well as data breach notification obligations for telco operators.

**Forecast for the proposed European ePrivacy Regulation**
On 10 January 2017, the European Commission published a draft for new EU ePrivacy Regulation, which shall replace the above-mentioned ePrivacy Directive.

In the draft, there are a few changes to the current rules. For example, over-the-top communications providers, instant messaging services and Voice over Internet Protocol providers now will also fall within the scope of these sector-specific data protection rules.

In principle, all electronic communications data (i.e., electronic communications content and electronic communications metadata) shall be confidential, and any interference, including surveillance or processing of electronic communications data, shall be prohibited, except when permitted by the ePrivacy Regulation. The following exceptions set out in Art. 6 of the ePrivacy Regulation (draft) are currently very limited, which might have an impact on business models, especially for OTT communications services, which are often financed by means of analyzing or selling customer data.

The rules of the ePrivacy Regulation (draft) shall apply to the provision of electronic communications services (ECS) to end users in the EU, irrespective of whether a payment of the end user is required.

ECS providers not established in the EU shall designate a representative within the EU who has the power to answer questions and provide information, in particular to supervisory authorities and end users.
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY’s Global Telecommunications Sector
Telecommunications operators are facing a rapidly transforming business model. Competition from technology companies is creating challenges around customer ownership. Service innovation, pricing pressures and network capacity are intensifying scrutiny of the return on investments. In addition, regulatory pressures and shareholder expectations require agility and cost efficiency. If you are facing these challenges, we can provide a sector-based perspective on addressing your assurance, advisory, transaction and tax needs. Our Global Telecommunications Sector is a virtual hub that brings together people, cultures and leading ideas from across the world. Whatever your need, we can help you improve the performance of your business. For more information, visit ey.com/telecommunications.

This news release has been issued by EYGM Limited, a member of the global EY organization that also does not provide any services to clients.

© 2017 Ernst & Young LLP.
All Rights Reserved.

EYG no. 03868-174Gbl
1703-2218295
ED None.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.