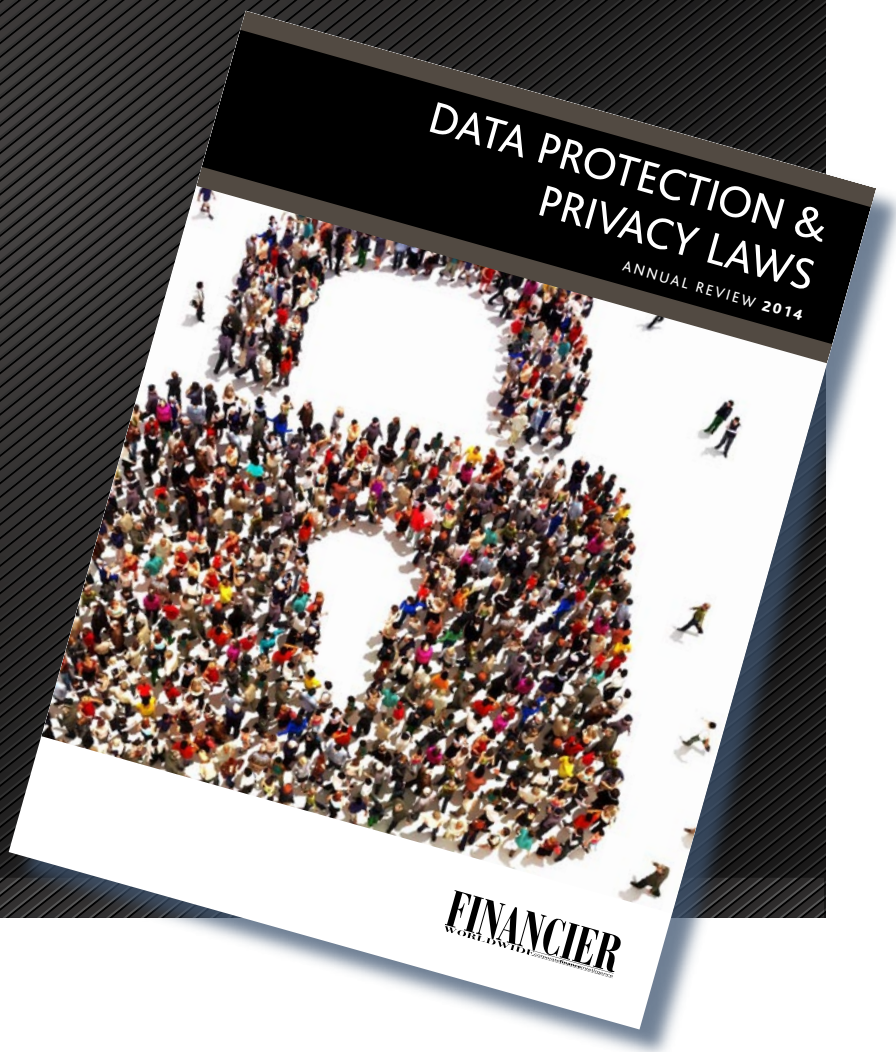
ANNUAL REVIEW

Data Protection & Privacy Laws



REPRINTED FROM
ONLINE CONTENT
NOVEMBER 2014

PREPARED ON BEHALF OF

HUNTON& WILLIAMS

FINANCIER WORLDWIDE corporatefinanceintelligence

UNITED KINGDOM

BRIDGET TREACY
HUNTON & WILLIAMS LLP

Q IN YOUR EXPERIENCE, DO COMPANIES PAY ENOUGH ATTENTION TO THE RISKS ASSOCIATED WITH DATA PROTECTION? ARE THEY BEGINNING TO FULLY UNDERSTAND THEIR DUTIES OF CONFIDENTIALITY AND PRIVACY IN THE DIGITAL AGE?

TREACY: Companies vary considerably in their approach to managing data protection risk. In my experience, it is the enlightened few that have a comprehensive, risk-based approach to data protection compliance. Often these are companies that operate in regulated industries, with well-structured risk management procedures deeply embedded within the corporate culture, or companies that have experienced a data security breach or regulatory enforcement. Too many companies still overlook data privacy issues, or focus their attention too narrowly on data security, ignoring the numerous other aspects of data protection compliance. In a world of big data analytics, the cloud, and the internet of things, the businesses that flourish are those that use their data assets strategically, and build consumer trust in their use of data. As we move towards the adoption of the proposed General Data Protection Regulation in Europe, with its detailed compliance requirements and significantly greater fines – 2-5 percent of global turnover – companies are starting to focus more closely on managing data protection risk.

Q COULD YOU OUTLINE THE LATEST LEGAL AND REGULATORY DEVELOPMENTS AFFECTING CORPORATE STORAGE, HANDLING AND TRANSFER OF DATA IN THE UK?

TREACY: In the UK, we have seen a growing focus on the security of personal data, whether in storage or in transit, and whether handled by the company itself or by third party services providers. Increasingly, the storage, handling and transfer of data takes place in a cloud environment. UK and other European regulators have been quick to emphasise that the usual rules of data protection still apply to data processed in the cloud, yet many companies overlook the need for their services agreements with cloud vendors to comply with basic data protection requirements. There is also a growing focus on data sharing, and on the permitted uses of personal data, particularly in the context of big data analytics. Organisations need to plan their data processing activities with care – just because the data can be collected does not mean it can be used at will.

Q IN WHAT WAYS HAVE GLOBAL AUTHORITIES INCREASED THEIR MONITORING AND ENFORCEMENT ACTIVITIES WITH RESPECT TO DATA PROTECTION AND PRIVACY IN RECENT YEARS?

TREACY: Although data privacy is a global issue, regulatory enforcement is local. Where data privacy issues affect individuals in multiple countries, we have seen an increase in informal cooperation and information sharing between national data protection authorities. More formally, the Global Privacy Enforcement Network was formally launched in July 2010 specifically to share information about enforcement issues, trends and experiences, and to facilitate training, cross-border privacy enforcement and complaint resolution. Although the network has no formal powers, it has led to regulators collaborating to examine specific aspects of compliance globally. More than 50 privacy regulators have joined the network, with the US Federal Trade Commission one of the founding members and the US Federal Communications Commission joining in October 2014. At a national level, regulators are gaining additional powers, usually to conduct audits and impose monetary penalties or fines. These trends towards coordination and more meaningful sanctions are reflected in the Proposed EU General Data Protection Regulation, where fines of 2-5 percent of global turnover are currently under discussion.

Q WHAT INSIGHTS CAN WE DRAW FROM RECENT HIGH-PROFILE DATA BREACHES? WHAT IMPACT HAVE THESE SITUATIONS HAD ON THE DATA PROTECTION LANDSCAPE?

TREACY: Data breaches are ubiquitous, and come in all shapes and sizes, although a surprising number of companies still maintain that they have never suffered a breach. Failure to acknowledge and proactively address this growing threat is a worrying trend. Although breach reporting is not a mandatory legal requirement in the UK, it is strongly encouraged by the UK data protection authority. Certainly, the UK has had its share of data breaches, although many do not reach the public domain. Many recent high profile examples involve external intruders or hackers, but all too often breaches are caused by 'insiders' – disillusioned employees, contract staff or outsource service providers, or staff who simply make mistakes. We have also seen an increase in cyber threats, particularly those targeted at critical infrastructure, and legislative attempts to

address the threat. At a practical level, we have worked with clients to prepare breach response plans, but also to stress-test or rehearse these response plans. Increasingly, we see these initiatives led by the board.

Q THE USE OF THIRD PARTIES, SUCH AS CONSULTANTS, AGENTS AND DISTRIBUTERS, EXPOSES FIRMS TO UNIQUE DATA PROTECTION RISKS. WHAT ARE SOME OF THESE RISKS AND WHAT STEPS CAN BE TAKEN TO MITIGATE THEM?

TREACY: The risk inherent in using third parties to process data is often overlooked. Recent breach incidents that we have advised on have involved rogue staff at an outsourced call centre operation, rogue contract staff with full access to confidential data, inadvertent sharing of sensitive data due to systems upgrades by contract staff, and the failure of several companies to conduct adequate diligence or negotiate adequate contractual terms with their cloud vendors. Organisations need to recognise that sharing personal data with third parties is a significant area of weakness. Taking simple steps to recognise when data are being shared with a third party, conducting basic diligence, including contractual safeguards, and implementing processes to monitor how personal data are used by the third party can significantly reduce data protection risk. Organisations that choose to use a third party to process data still retain legal responsibility for that data, and should expect to be investigated in the event of a data breach.

Q WHAT CAN COMPANIES DO TO MANAGE INTERNAL DATA PRIVACY RISKS AND THREATS, SUCH AS LIABILITIES ARISING FROM LOST DEVICES OR THE ACTIONS OF ROGUE EMPLOYEES?

TREACY: Companies need to promote a good level of awareness among their staff of data privacy risks and threats. Rules or policies that define acceptable and unacceptable behaviour are important, but are not sufficient by themselves. It is crucial that staff can recognise incidents, and know where to report their concerns promptly. In the UK there have been several data breaches where organisations have been penalised further by regulators because their internal breach response processes were inadequate. Practical steps should be taken to encrypt portable devices, and to ensure that arrangements for remote working and BYOD do not compromise the security of personal data. Companies should also review their exit procedures. There are numerous cases of employees – not all of whom are disgruntled – taking a copy of the client database when they leave.

"Organisations that choose to use a third party to process data still retain legal responsibility for that data, and should expect to be investigated in the event of a data breach."

Q WHAT ADVICE CAN YOU OFFER TO COMPANIES ON MANAGING DATA RISK, INSTALLING INTERNAL COMPLIANCE PROCESSES AND MAINTAINING COMPLIANCE ON DATA PRIVACY GOING FORWARD?

TREACY: Increasingly, personal data is a business' most valuable asset. Data security is crucial to safeguard those assets, but in a world of big data analytics, the cloud, and the internet of things, the businesses that flourish will be those that use their data assets strategically. To do that, companies need to start with the basics and know what data they hold, how it was collected, from whom, and on what basis. They need to think strategically about the creation and collection of data, what they would like to use the data for, and what expectations individuals might have about data use. They need to be transparent and build consumer trust in their use of data. Crucially, they need to be able to demonstrate compliance with privacy laws, utilising policies, procedures such as Privacy Impact Assessments, and people, including data protection officers. These are strategic objectives that need to be brought to life within the culture of an organisation.

HUNTON& WILLIAMS

Bridget Treacy

Partner
Hunton & Williams LLP
T: +44 (0)20 7220 5731
E: btreacy@hunton.com

Bridget Treacy leads Hunton & Williams' UK Privacy and Cybersecurity team. For more than 14 years her practice has focused on all aspects of privacy and information governance for multinational companies, including big data analytics and the internet of things, behavioural targeting, cloud computing, cross-border data transfers and BCRs, and data breach. Ms Treacy is top ranked in Chambers, which describes her as "one of the leading thinkers on data protection, providing practical solutions to thorny legal issues".

FRANCE

CLAIRE FRANÇOIS
HUNTON & WILLIAMS LLP

Q IN YOUR EXPERIENCE, DO COMPANIES PAY ENOUGH ATTENTION TO THE RISKS ASSOCIATED WITH DATA PROTECTION? ARE THEY BEGINNING TO FULLY UNDERSTAND THEIR DUTIES OF CONFIDENTIALITY AND PRIVACY IN THE DIGITAL AGE?

FRANÇOIS: Companies are definitely paying more attention to the risks associated with data protection, including reputational risks. This may be explained by a number of factors, and in particular, the increased publicity around privacy and data protection. The French data protection authority (CNIL) makes most of its decisions public and the media increasingly reports on privacy and data protection issues, such as the recent ruling of the Court of Justice acknowledging the right to be 'de-listed' from the list of results displayed by search engines. Companies are all the more paying attention to the risks associated with data protection in view of the proposed changes to the EU regulatory framework for data protection – in particular, the proposal to increase the maximum level of fines to 5 percent of a company's annual worldwide turnover in the draft General Data Protection Regulation. This prompts companies to better understand their data protection obligations under the current and new proposed regulatory framework.

Q COULD YOU OUTLINE THE LATEST LEGAL AND REGULATORY DEVELOPMENTS AFFECTING CORPORATE STORAGE, HANDLING AND TRANSFER OF DATA IN FRANCE?

FRANÇOIS: Companies operating a whistleblowing scheme in France have to register their scheme with the CNIL either by self-certifying to the CNIL's Single Authorization AU-004 decision, or by filing a formal request for approval with the CNIL. On 30 January 2014, the CNIL broadened the scope of its Single Authorization AU-004 so as to include whistleblowing schemes implemented to fight against discrimination and harassment in the workplace or to ensure health, hygiene and security in the workplace and/or protection of the environment. Companies that have already self-certified to the CNIL's Single Authorization AU-004 can now extend the scope of their whistleblowing schemes to these areas. Compliance with cookie law requirements has also been a priority for the CNIL. On 5 December 2013, the CNIL issued new guidelines on cookies and similar technologies, and decided to conduct inspections – which started in October 2014 – to verify whether companies comply with these new guidelines.

Q IN WHAT WAYS HAVE GLOBAL AUTHORITIES INCREASED THEIR MONITORING AND ENFORCEMENT ACTIVITIES WITH RESPECT TO DATA PROTECTION AND PRIVACY IN RECENT YEARS?

FRANÇOIS: The CNIL's monitoring and enforcement activities have increased in a number of ways. First, a French consumer law of 17 March 2014 has strengthened the CNIL's investigative powers by giving it the ability to conduct online inspections. This new investigative power has triggered a higher number of inspections: the CNIL has set itself the objective of conducting about 550 inspections in 2014, which would be an increase of 13 percent compared to 2013. Last but not least, the CNIL actively took part in joint online audit actions in May 2013 and 2014 in the context of Global Privacy Enforcement Network's (GPEN's) first and second annual enforcement sweeps and in September 2014 in the context of the European 'cookies sweep day' initiative.

Q WHAT INSIGHTS CAN WE DRAW FROM RECENT HIGH-PROFILE DATA BREACHES? WHAT IMPACT HAVE THESE SITUATIONS HAD ON THE DATA PROTECTION LANDSCAPE?

FRANÇOIS: Recent high-profile data breaches show that a company affected by a data breach remains liable for that breach if it is the data controller – meaning the entity that determines the purposes and means of the data processing – even if the breach is attributable to a third party. On 12 June 2014, the CNIL imposed a sanction, or public warning, against the French affiliate of transportation company DHL for failing to ensure the security and confidentiality of customer personal data, following a data breach due to a design defect attributable to a service provider. On 7 August 2014, the CNIL imposed the same sanction against the French telecommunications service provider, Orange, in a case where the breach was due to a technical failure of one of Orange's service providers. These recent high-profile data breaches also recall that, as data controllers, companies must ensure compliance not only with data security requirements but also with any other data protection requirement, such as data retention limitations.

FRANCE • CLAIRE FRANÇOIS • HUNTON & WILLIAMS LLP

"Companies should closely monitor any EU and national developments with respect to privacy and data protection, as the regulatory framework is constantly evolving."

Q THE USE OF THIRD PARTIES, SUCH AS CONSULTANTS, AGENTS AND DISTRIBUTERS, EXPOSES FIRMS TO UNIQUE DATA PROTECTION RISKS. WHAT ARE SOME OF THESE RISKS AND WHAT STEPS CAN BE TAKEN TO MITIGATE THEM?

FRANÇOIS: The use of third parties for the processing of personal data entails the risk that the data are used for purposes other than those for which it was collected and the security and confidentiality of the data are not protected – as shown by recent data breaches. EU and French data protection law requires that any company that subcontracts part or all of its data processing activities conclude a written agreement with the subcontractor specifying that the latter must act only on the instructions of the company – the data controller – and implement appropriate technical and organisational security measures. The conclusion of such agreement or the insertion of appropriate data protection language in a service agreement helps to mitigate the above risks. In addition, companies should carry out regular and complete security audits of their own data processing facilities and those of their subcontractors.

Q WHAT CAN COMPANIES DO TO MANAGE INTERNAL DATA PRIVACY RISKS AND THREATS, SUCH AS LIABILITIES ARISING FROM LOST DEVICES OR THE ACTIONS OF ROGUE EMPLOYEES?

FRANÇOIS: Companies can first reduce these risks and threats by having a deep and up-to-date understanding of their own data processing activities – for example, the types of data they process, the purposes for which the data is processed, the data recipients, and so on – by making sure that they have the proper legal data transfer mechanisms and data processing agreements in place, and by complying with all the necessary registrations with the CNIL. Companies should also implement internal policies on how to use personal data of, for example, job applicants, employees, customers and vendors, and keep it secure, including what to do in case of a data breach. More generally, companies should raise employee awareness about privacy and data protection requirements, for instance through training activities.

Q WHAT ADVICE CAN YOU OFFER TO COMPANIES ON MANAGING DATA RISK, INSTALLING INTERNAL COMPLIANCE PROCESSES AND MAINTAINING COMPLIANCE ON DATA PRIVACY GOING FORWARD?

FRANÇOIS: Companies should closely monitor any EU and national developments with respect to privacy and data protection, as the regulatory framework is constantly evolving. Pending the revision of the EU regulatory framework, companies operating in France should rely on the CNIL's guidance to implement internal data protection compliance programs. The CNIL regularly issues specific and practical guidance on a variety of issues that can help companies to achieve and maintain such compliance. Although the appointment of a Data Protection Officer (DPO) is currently not mandatory in France, large companies may also consider appointing a DPO, whose main responsibility is to ensure compliance with French data protection requirements.

HUNTON& WILLIAMS

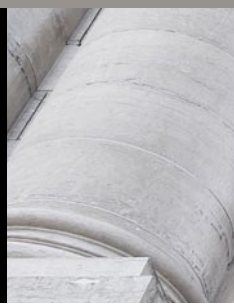
Claire François

Associate
Hunton & Williams LLP
+32 (0)2 643 58 00
cfrancois@hunton.com

Claire François is a French qualified lawyer and advises a broad spectrum of clients on EU and French data protection and cyber security matters, including implementation of global data management strategies, international data transfers, and local data compliance. She also regularly represents clients before the French Data Protection Authority.

BELGIUM

WIM NAUWELAERTS
HUNTON & WILLIAMS LLP



Q IN YOUR EXPERIENCE, DO COMPANIES PAY ENOUGH ATTENTION TO THE RISKS ASSOCIATED WITH DATA PROTECTION? ARE THEY BEGINNING TO FULLY UNDERSTAND THEIR DUTIES OF CONFIDENTIALITY AND PRIVACY IN THE DIGITAL AGE?

NAUWELAERTS: In my experience, many companies are still underestimating the risks of not complying with data protection rules, in particular the potential reputational harm that may result from such non-compliance. However, data protection compliance is slowly moving up the agenda of companies with business operations in Belgium, for a number of reasons. Individuals are becoming more vocal when it comes to the protection of their privacy and personal data, which is evidenced by an increasing number of data access requests and complaints submitted to the Belgian data protection authority – the Privacy Commission. Former employees seem more eager to invoke privacy and data protection issues when fighting their dismissal in court. The media is also increasingly paying attention to privacy and data protection issues, such as data breaches and cyber monitoring, which prompts companies to heighten internal awareness of privacy and data protection requirements. Last but not least, the proposed changes to the EU data protection framework – in particular the European Commission's draft General Data Protection Regulation – will raise the bar for companies in terms of compliance requirements. Many companies are closely following the discussions around the General Data Protection Regulation, which is expected to be adopted in the first half of next year, with a view to assessing their current level of compliance.

Q COULD YOU OUTLINE THE LATEST LEGAL AND REGULATORY DEVELOPMENTS AFFECTING CORPORATE STORAGE, HANDLING AND TRANSFER OF DATA IN BELGIUM?

NAUWELAERTS: The most important development is probably that since 1 September 2014, consumers who have suffered damage as a result of a violation of the Belgian data protection act are able to initiate class action proceedings before the Belgian courts. Consumers cannot bring such action themselves – they must appoint a representative for that purpose, such as an association. It is expected that the introduction of this collective redress possibility will trigger more court proceedings based on data protection law infringements. The Belgian Privacy Commission recently

introduced notification forms to report data security breaches. There is currently no general obligation in Belgium to report data security breaches: the Electronic Communications Act of 13 June 2005 – *Wet betreffende de elektronische communicatie* – imposes a duty to notify, but this applies only to providers of electronic communications services. However, the Privacy Commission generally advises companies to report data security breaches to the competent authorities within 48 hours, and has now issued specific forms for that purpose. In addition, the Privacy Commission has published guidance on data processing associated with the use of apps, drones, and dashboard-mounted cameras. The Privacy Commission has further endorsed the recent publication, by the Belgian Cybercrime Centre, of the first Belgian Cyber Security Guide, which sets out key security principles and 'must-do' actions for companies facing cyber risks. The guide is important because non-compliance may be considered by the Privacy Commission as an indication of insufficient data security – for example, in the event of a cyber incident.

Q IN WHAT WAYS HAVE GLOBAL AUTHORITIES INCREASED THEIR MONITORING AND ENFORCEMENT ACTIVITIES WITH RESPECT TO DATA PROTECTION AND PRIVACY IN RECENT YEARS?

NAUWELAERTS: Data protection authorities, including the Belgian Privacy Commission, are increasingly combining forces, in particular in the context of the activities of the Global Privacy Enforcement Network (GPEN). GPEN was established in 2010 with the aim of ensuring cooperation between data protection authorities in the field of cross-border data protection law enforcement. It provides a platform for data protection authorities to share best practices in addressing cross-border challenges and exchange information on particular enforcement cases. Last May, GPEN carried out a general investigation or 'sweep' to assess mobile app compliance with data protection laws. Twenty-six data protection authorities worldwide evaluated 1211 mobile apps and found that a large majority of the apps were accessing personal data without providing adequate information to users. GPEN is likely to conduct more 'sweeps' in the future.

Q WHAT INSIGHTS CAN WE DRAW FROM RECENT HIGH-PROFILE DATA BREACHES? WHAT IMPACT HAVE THESE SITUATIONS HAD ON THE DATA PROTECTION LANDSCAPE?

NAUWELAERTS: In light of the recent rise in high-profile data breaches – including the National Belgian Railway Company and the Belgian Ministry of Defense – the Belgian Privacy Commission has issued specific guidance on data security and working with computer files in particular: *Aanbeveling nr. 1/2013,* dated 21 January 2013. Companies subject to Belgian data protection law are expected to evaluate their data security measures in light of the Privacy Commission's guidance. Failure to do so could trigger liability under the Belgian Data Protection Act in the event of a data breach.

Q THE USE OF THIRD PARTIES, SUCH AS CONSULTANTS, AGENTS AND DISTRIBUTERS, EXPOSES FIRMS TO UNIQUE DATA PROTECTION RISKS. WHAT ARE SOME OF THESE RISKS AND WHAT STEPS CAN BE TAKEN TO MITIGATE THEM?

NAUWELAERTS: There are several data protection risks associated with the use of third-party 'data processors' such as consultants, agents and distributors. For instance, if data processors use the personal data entrusted to them for their own business purposes in violation of data protection rules, the 'data controllers' that initially provided the data can be held responsible. Data controllers also have to make sure that any third-party 'data processors' they involve in handling personal data have implemented appropriate technical and organisational measures to keep the data secure. Data processors should not transfer personal data outside of the European Economic Area unless there is a valid legal mechanism for doing so. In addition, in the event of a data breach, it is essential that data controllers are immediately informed by their third-party data processors so that they can properly evaluate the situation and take remedial action. In order to mitigate the risks on the part of data controllers, there should be data protection clauses in the agreements with third-party data processors that address these risks in detail.

Q WHAT CAN COMPANIES DO TO MANAGE INTERNAL DATA PRIVACY RISKS AND THREATS, SUCH AS LIABILITIES ARISING FROM LOST DEVICES OR

NAUWELAERTS: Companies can substantially reduce such risks and threats by making sure that they comply with the 'basic' obligations imposed by Belgian data protection rules. For example, companies should ensure that they have submitted registrations for their data processing activities with the Belgian Privacy Commission, where required. They should also provide adequate privacy notices to employees – to inform them about, for instance, any employee monitoring at the workplace – and adopt internal policies

"For companies doing business in Belgium, the Belgian Privacy Commission's guidance plays an increasingly important role in shaping companies' compliance processes and programs."

THE ACTIONS OF ROGUE EMPLOYEES?

and standard operating procedures on how to use employees' personal data and keep it secure.

Q WHAT ADVICE CAN YOU OFFER TO COMPANIES ON MANAGING DATA RISK, INSTALLING INTERNAL COMPLIANCE PROCESSES AND MAINTAINING COMPLIANCE ON DATA PRIVACY GOING FORWARD?

NAUWELAERTS: For companies doing business in Belgium, the Belgian Privacy Commission's guidance plays an increasingly important role in shaping companies' compliance processes and programs. As the Privacy Commission issues more specific guidance on a variety of topics, it is advisable for companies to monitor this guidance and, if applicable, adapt their practices accordingly. In addition, any company that handles personal data should start assessing to what extent the EU's new regulatory framework for data protection – that is, the General Data Protection Regulation – will impact the way in which it collects, processes and transfers personal data. Although there will be a two-year transition period before the new rules kick in, the sooner companies engage in this assessment, the better.

HUNTON& WILLIAMS

Wim Nauwelaerts

Partner
Hunton & Williams LLP
+32 02 643 5800
wnauwelaerts@hunton.com

Wim Nauwelaerts leads Hunton & Williams' Privacy and Cyber Security team in Brussels. His practice focuses on European data protection matters, with a particular emphasis on privacy issues in the areas of new media and communication technologies, financial services, healthcare and life sciences. Mr Nauwelaerts is recognised as a leading privacy practitioner by *Chambers Global*, *The Legal 500 (Belgium)*, and *The International Who's Who of Technology Lawyers*. He has written and spoken widely on privacy-related topics, such as cloud computing.

CHINA & HONG KONG

MANUEL MAISOG
HUNTON & WILLIAMS LLP

Q IN YOUR EXPERIENCE, DO COMPANIES PAY ENOUGH ATTENTION TO THE RISKS ASSOCIATED WITH DATA PROTECTION? ARE THEY BEGINNING TO FULLY UNDERSTAND THEIR DUTIES OF CONFIDENTIALITY AND PRIVACY IN THE DIGITAL AGE?

MAISOG: In Mainland China, it is hard to give a single consistent answer because China's data privacy framework is emerging on a patchwork, sector-by-sector basis. As such, companies in some sectors are becoming aware of the risks and duties associated with collecting and handling personal information, while companies in other sectors have little awareness of the same risks and little incentive to develop any awareness of them. On the whole, however, it is probably true that companies in Mainland China are not as aware of the risks and duties associated with personal information as they should be. Chinese government authorities, however, are improving their knowledge and skills in formulating and enforcing the nation's privacy and data protection rules. Repeated enforcement campaigns, in which suspects are rounded up for investigations seemingly in wholesale waves, as well as repeatedly reactive rulemaking – in which regulations are promulgated only after and in response to an event or crisis – seem to suggest weaknesses in the overall attitude with which privacy-related risks are regarded in China.

Q COULD YOU OUTLINE THE LATEST LEGAL AND REGULATORY DEVELOPMENTS AFFECTING CORPORATE STORAGE, HANDLING AND TRANSFER OF DATA IN CHINA & HONG KONG?

MAISOG: The very latest development in Mainland China is a Supreme Court interpretation that prohibits the disclosure of personal information over information networks, including the internet. This allows for exceptions, such as where the data subject has consented or where the disclosure is in the national interest. Another significant recent development is a regulation that imposes security safeguard requirements on the handling of personal health information. Importantly, this imposes a cross-border transfer restriction, in which entities involved in health care are prohibited from transferring personal health information to servers located outside of China. Other interesting developments involve regulations which require postal and courier service providers to adopt security safeguards, or impose discipline on employees of life insurance companies that misappropriate the personal information of policyholders, in an attempt to prevent the information-processing functions within these business sectors from becoming points of leakage.

Q IN WHAT WAYS HAVE GLOBAL AUTHORITIES INCREASED THEIR MONITORING AND ENFORCEMENT ACTIVITIES WITH RESPECT TO DATA PROTECTION AND PRIVACY IN RECENT YEARS?

MAISOG: In China, government authorities are paying more and more attention to privacy and data protection. In newly promulgated data protection rules, data breach activities are subject to substantial monetary compensation, administrative penalties and even criminal liabilities. For example, in the recent Supreme Court interpretation, the Supreme Court specified that the compensation awarded by a court to a victim of an infringement of personal rights may reach RMB 500,000. Also, in the Consumer Rights Protection Law, a business operator which infringes upon a consumer's personal information may forfeit the illegal income and be subject to a fine of up to 10 times the illegal income – or, if there is no illegal income, the fine may range up to RMB 500,000. In addition, recently there was a criminal conviction in a Shanghai court of a British-American couple who had been accused of committing illegal collection of personal information in the course of conducting their investigatory consulting business.

Q WHAT INSIGHTS CAN WE DRAW FROM RECENT HIGH-PROFILE DATA BREACHES? WHAT IMPACT HAVE THESE SITUATIONS HAD ON THE DATA PROTECTION LANDSCAPE?

MAISOG: Foreigners now must view themselves as not immune from investigation or prosecution for improper handling of personal information in China. This will cause some foreign entities doing business in China to act much more cautiously when investigating prospective business partners in China.

Q THE USE OF THIRD PARTIES, SUCH AS CONSULTANTS, AGENTS AND DISTRIBUTERS, EXPOSES FIRMS TO UNIQUE DATA PROTECTION RISKS.

MAISOG: In the context of Mainland China, the third-party consultant risk can arise from third party investigators who are hired to conduct due diligence investigations. The conviction of the British-American couple in Shanghai shows that the performance of these services can, if not conducted carefully, involve the risk of criminal liability. To mitigate these risks, one possibility is simply not to hire a third-party investigatory firm at all, or at least not to

WHAT ARE SOME OF THESE RISKS AND WHAT STEPS CAN BE TAKEN TO MITIGATE THEM?

hire one whose practices and tactics one does not already fully understand. Another possibility is to restrict investigation to information that is already publicly available without controversy; a recent reform of the administration of companies and corporate information – started by an order of the State Council in February 2014 – makes a wide range of corporate information publicly available, and in some cases beyond what is required in the US to be publicly available, and a firm may want to view this information first to decide if it may be sufficient in and of itself. Another possibility is to specifically instruct that in any investigation, no personal information may be handled – that is, only non-personal business information should be handled, such as photographs that evidence infringements of intellectual property rights, information on production activities, to the extent this can be structured so as not to violate antitrust laws.

Q WHAT CAN COMPANIES DO TO MANAGE INTERNAL DATA PRIVACY RISKS AND THREATS, SUCH AS LIABILITIES ARISING FROM LOST DEVICES OR THE ACTIONS OF ROGUE EMPLOYEES?

MAISOG: In the context of Mainland China, the management of internal privacy risks would not be particularly different from how it would be conducted in other jurisdictions. There are no particular rules on how employee monitoring should be conducted, although there are few general rules on privacy and personal information protection, and employers are in any event required to keep their employees' personal data in confidence and to obtain the relevant employee's written consent before disclosing his or her personal data.

Q WHAT ADVICE CAN YOU OFFER TO COMPANIES ON MANAGING DATA RISK, INSTALLING INTERNAL COMPLIANCE PROCESSES AND MAINTAINING COMPLIANCE ON DATA PRIVACY GOING FORWARD?

MAISOG: You should handle personal information with respect and care, even if you are operating in an industry sector for which a rigorous or detailed data privacy framework has not yet been implemented. The laws and regulations are emerging rapidly, and unpredictably, enough in China that committing yourself to and investing in a business model that relies on data handling methods that are suddenly ruled improper can prove to be awkward or even, as the British-American couple in Shanghai discovered, painful. In fact, you should learn to handle personal information with respect and care, even if you are operating in a country that has no data privacy law. The internet has made the world a smaller place, and because they

"You should handle personal information with respect and care, even if you are operating in an industry sector for which a rigorous or detailed data privacy framework has not yet been implemented."

have the practical effect of earning consumer trust, respectful data handling practices have the potential to be a competitive advantage even in places where not legally required. Even in a country that has no data privacy law at all, a business model that is firmly rooted in aggressive or loose personal information handling practices may one day find itself at a competitive disadvantage once an international business operator, versed in respectful but commercially efficient data handling practices developed in marketplaces where data privacy laws have to be observed, arrives to compete in the same territory.

HUNTON& WILLIAMS

Manuel Maisog

Partner
Hunton & Williams LLP
+86 10 5863 7507
bmaisog@hunton.com

Bing Maisog is the Chief Representative of the firm's office in Beijing. He is a member of the firm's Corporate practice team, and has also worked as a member of the Energy and Infrastructure team. Prior to the establishment of the Beijing office, he was resident in both Bangkok and Hong Kong, and worked on significant project finance and project acquisition transactions in many countries across Asia. In the past, he has also worked as a corporate finance lawyer, with experience in initial public offerings, private placements, and financial institution merger and acquisition transactions.

www.financierworldwide.com