GLOBAL

The Future of Data Privacy

As we enter the age of artificial intelligence and the Internet of Things, our personal data matters more than ever. In the following global guide you'll hear from 23 legal experts from across the globe about how data privacy laws are changing in response to GDPR.

IR Global - The Future of Professional Services

IR Global was founded in 2010 and has since grown to become the largest practice area exclusive network of advisors in the world. This incredible success story has seen the network awarded Band 1 status by Chamber & Partners, featured in Legal 500 and in publications such as The Financial Times, Lawyer 360 and Practical Law, among many others.

The group's founding philosophy is based on bringing the best of the advisory community into a sharing economy; a system that is ethical, sustainable and provides significant added value to the client.

Businesses today require more than just a traditional lawyer or accountant. IR Global is at the forefront of this transition, with members providing strategic support and working closely alongside management teams to help realise their vision. We believe the archaic 'professional service firm' model is dying due to it being insular, expensive and slow. In IR Global, forward-thinking clients now have a credible alternative, which is open, cost effective and flexible.

Our Founding Philosophies

Multi-Disciplinary

We work alongside legal, accountancy, financial, corporate finance, transaction support and business intelligence firms, ensuring we can offer complete solutions tailored to the client's requirements.

Niche Expertise

In today's marketplace, both local knowledge and specific practice area/sector expertise is needed. We select just one firm, per jurisdiction, per practice area ensuring the very best experts are on hand to assist.

Vetting Process

Criteria is based on both quality of the firm and the character of the individuals within. It's key that all of our members share a common vision towards mutual success.

Personal Contact

The best relationships are built on trust and we take great efforts to bring our members together via regular events and networking activities. The friendships formed are highly valuable to the members and ensure client referrals are handled with great care.

Co-Operative Leadership

In contrast to authoritarian or directive leadership, our group puts teamwork and self-organisation in the centre. The group has steering committees for 12 practice area and regional working groups that focus on network development, quality controls and increasing client value.

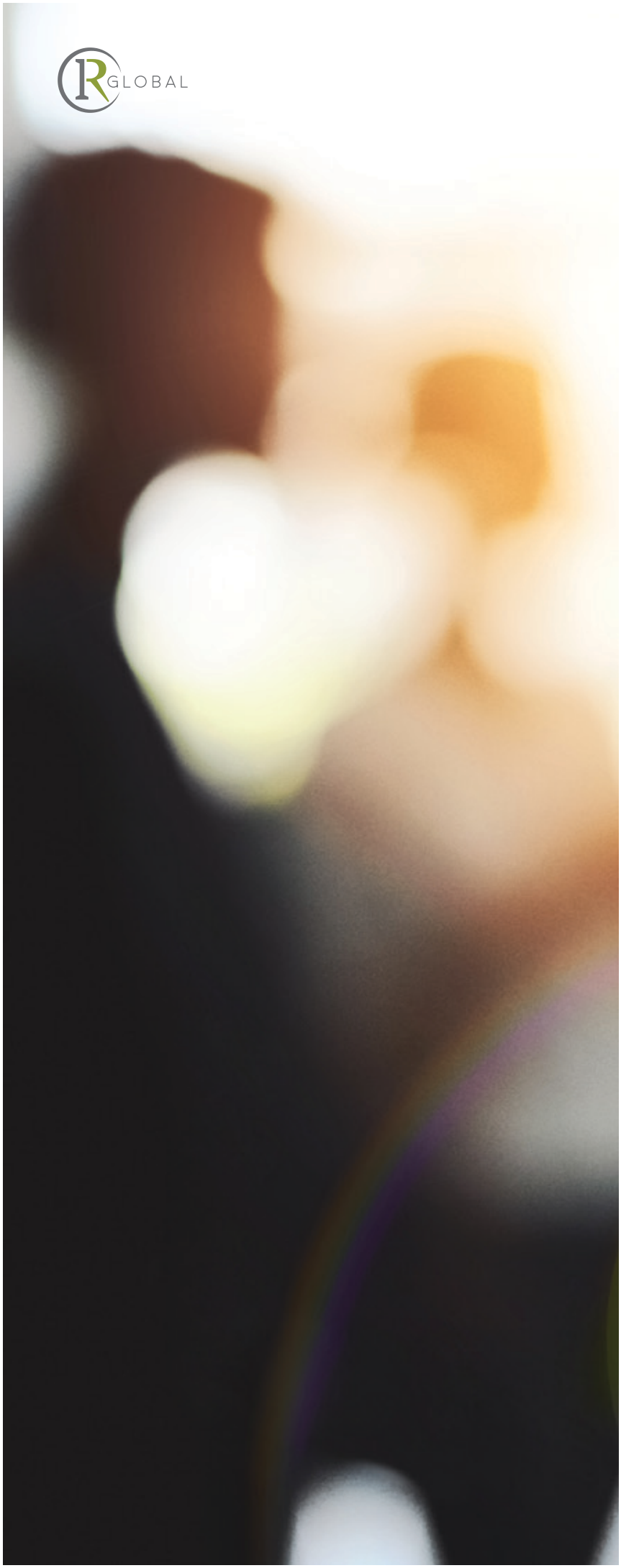
Ethical Approach

It is our responsibility to utilise our business network and influence to instigate positive social change. IR Global founded Sinchi, a non-profit that focuses on the preservation of indigenous culture and knowledge and works with different indigenous communities/tribes around the world.

Strategic Partners

Strength comes via our extended network. If we feel a client's need is better handled by someone else, we are able to call on the assistance of our partners. First priority is to always ensure the client has the right representation whether that be with a member of IR Global or someone else.

Rachel Finch
IR Global - Channel Sales Manager
rachel@irglobal.com



Contributors

FOREWORD BY EDITOR, ANDREW CHILVERS

Tighter Regulations Needed for the Global Data Tsunami

As we enter the age of artificial intelligence and the Internet of Things, our personal data matters more than ever.

By the mid-2020s, all devices will be creating 163 zettabytes of data a year. That's the same as viewing all the movies on Netflix more than 500 million times; it's an increase of 10 times the current yearly data creation rate of 16.3ZB.

Given these extraordinary statistics, the General Data Protection Regulation (GDPR), introduced in May 2018, was set up to regulate this largely unregulated data universe. The idea was to instil vital compliance by organisations, brands and social media companies often viewed by consumers as exploiting their data in nefarious ways.

Although it's only been just over a year, people are starting to understand the far-reaching implications of the regulations. Some organisations – from large online retailers to healthcare providers – are already implementing the necessary procedures for compliance. But almost a third of EU organisations – public and private sector – still lag behind when it comes to complying with GDPR. Globally, the figure for non compliance with the different data protection regulations in each country is far worse – some estimates put it as high as 80%.

Under GDPR, the maximum fine for a company hit with a data breach is £17 million or 4% of global turnover, whichever is greater. Recently, in the Marriott Hotel Group was fined almost £100m by the UK Information Commissioner's Office (ICO) after hackers stole the records of 339 million guests. British Airways was also fined £183m when 500,000 customer data records were breached. So the UK's ICO has taken a lead in ensuring that organisations understand the implications for non compliance of the regulations.

To highlight the success of the ICO's general awareness campaigns, in just a few months after the introduction of GDPR last May, data breach complaints increased 160% in the UK as British businesses came under more scrutiny from regulators and customers alike. By December, for many organisations alarm bells were ringing that data protection should now be taken much more seriously. Just one look at the ICO's website on recent data breaches gives a good indication of the rise in cyber attacks across all sectors – and the actions being taken.

And it's not just fines that will impact organisations - failing to comply will have a huge impact on reputational damage. In recent studies, 19% of British consumers said they would stop purchasing with a retailer if the company had been hacked. According to a 2018 UK Government report on cyber security, four in 10 UK businesses (43%) experienced a security breach or attack in the previous 12 months. These breaches cost small companies an average of £3,000 in productivity losses and reputational damage, while charges for medium-to-large businesses were estimated at more than £22,000, growing significantly year-on-year.

Globally, the EU's GDPR has without doubt become the benchmark of all data privacy legislations and has had a far-reaching impact on the global consensus around privacy; promoting greater transparency, acting as a catalyst in the incubation of similar laws and laying the onus on companies to protect user data.

In the following global guide you'll find evidence of this GDPR rippling effect across the world as we hear from legal experts from jurisdictions as far apart as California and New York, Mexico and Romania. Each legal advisor talks about how data privacy laws are changing in response to GDPR – and in some cases, ie, California, arguably going even further than the EU in data privacy.

Similarly, we will hear how different countries are driving privacy laws to suit their local environment – for both public and private sector – ensuring that all citizens feel more assured that state organisations and companies finally realise data privacy is everyone's business.

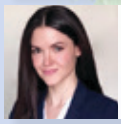
Andrew Chilvers
IR Global - Editor & Copywriter
andrew@irglobal.com

IR Global - Contributors by Region

IR Global Data Privacy experts aim to lead the industry and are at the forefront of the constantly developing legislation in their respective jurisdictions. They offer a full global Data Privacy offering, providing unrivaled knowledge no matter what the requirement and ensuring seamless international support to their clients. They are an asset to the IR Global network.

06. Aaron Allan
Partner, Glaser Weil Fink Howard Avchen & Shapiro LLP
irglobal.com/advisor/aaron-p-allan

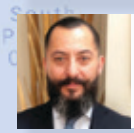
07. Alexander J. Suarez
Associate, Glaser Weil Fink Howard Avchen & Shapiro LLP
glaserweil.com/attorneys/alexander-suarez



18. Della M. Hill
Associate, MacDonald Weiss PLLC
irglobal.com/advisor/della-m-hill

13. Lavinia Junqueira
Partner, Junqueira Advogados
irglobal.com/advisor/lavinia-junqueira

14. Cauê Rodrigues Amaral
Associate, Junqueira Advogados
jlegalteam.com



15. Oscar Conde
Managing Partner, Legem Attorneys at Law, SC
irglobal.com/advisor/oscar-conde-medina

16. Dr. Juan José Rico Urbiola
Counseling/Compliance, Legem Attorneys at Law, SC
irglobal.com/advisor/juan-jose-rico

02. Jesszika Udvari
Partner, Buzády & Udvari Attorneys at law
irglobal.com/advisor/dr-jesszika-udvari

03. Monika Naef
Partner, DUFOUR Advokatur
irglobal.com/advisor/monika-naef

04. Robert Lewandowski
Partner, DLP Dr Lewandowski & Partners
irglobal.com/advisor/robert-lewandowski

05. Yusuf Mansur Özer
Associate, ErsoyBilgehan
irglobal.com/advisor/yusuf-mansur-oezer

08. Sönke Lund
Partner, Grupo Gispert
grupogispert.com/en/team/soenke-lund

09. Anna Fernqvist Svensson
Partner, hellström advokatbyrå kb
irglobal.com/advisor/anna-fernqvist-svensson

10. Matthew Lea
Senior Solicitor, Herrington Carmichael
herrington-carmichael.com/our-people/matthew-lea

11. Henrik Christian Strand
Associate Partner, Holst, Advokater
irglobal.com/advisor/henrik-christian-strand

12. Adelina Dospinescu
Managing Associate, Hristescu & Partners
hmpartners.ro/crew

17. Mohamed Agamy
Managing Partner, Links & Gains Law Firm
irglobal.com/advisor/mohamed-agamy

19. Dr. Dennis Voigt
Partner, MELCHERS Rechtsanwälte
irglobal.com/advisor/dr-dennis-voigt

23. Joost Peeters
Partner, STUDIO | LEGALE
irglobal.com/advisor/joost-peeters

01. Mark Benton
Partner, AHNSE Law Offices
irglobal.com/advisor/mark-benton

20. Divya Balagopal
Senior Partner, Mundkur Law Partners
mundkur.com

21. Nandita Bhakta
Counsel, Mundkur Law Partners
mundkur.com

22. Matthew Shearing
Associate, Rouse Lawyers
rouselawyers.com.au/our-team/matthew-shearing

KOREA

Mark Benton

Partner, AHNSE Law Offices

marktbenton@ahnse.com
irglobal.com/advisor/mark-benton
+82 2 743 0400

Mark is a Consultant to Ahnse law offices. He is an English solicitor currently non-practising. He began his career in the City of London with Abrahams Dresden Solicitors becoming a partner there before moving to rhw Solicitors. He has lived and worked in Asia since 2007, spending time in Indonesia before moving to South Korea.

Mark has worked with Ahnse since 2013 focussing on the firm's foreign clients – in bound and out bound. He works with a team of South Korean lawyers to provide advice on a broad range of commercial and legal issues. In his free time, Mark enjoys ultra endurance sports, literature and history.

ahnse.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

"Who controls the past controls the future. Who controls the present controls the past," wrote George Orwell in his seminal visionary work 1984 – a description of a dystopia, which was first published in 1949.

One wonders how much technology will have advanced in five let alone 10 years. 1984 made a resurgence in my early teens; its malevolent undertones remain just as relevant 70 years on.

Even the most perspicacious lawyer would be reticent to predict too far into the future. That said, the key challenges are clearly going to relate to the advancement of technology and how that will impinge on the relationship between the individual, corporations and the state.

Congress is already debating the future challenges of "big data" and the "IoT". This is bringing to the fore the competing interests of businesses which want greater access to data, and NGOs and academics who are concerned with the protection of the privacy of the individual.

Current issues include how encrypted data can and will be used, the impact of biotechnology and the use of secondary data deriving from personal information. There is also an ongoing debate about how financial information can and will be used. And the right to be forgotten and the "digital divide". These challenges are clearly analogous to those faced by other jurisdictions.

Perhaps on a more general level, we will need to start asking ourselves about what kind of people we actually want to be. The cornerstone of any liberal democracy is the rights of the individual. We are already addicted to and dependent on technology; to that extent, the genie is already out of the bottle. But how much do we want it to change us as people? A further issue is how we deal (and compete) with those who are less scrupulous with big data than ourselves.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

South Korea is a world leader in IT. It has one of the fastest, if not the fastest, internet speeds in the world. Its population is tech savvy and is constantly engaged on electronic devices and social media. It is natural therefore that the law as it pertains to privacy and the individual and data protection has been responsive to these changes. It has also evolved over time.

The first data protection legislation was enacted in 1995; it applied to government agencies only. The Constitutional Court determined in 2005 and confirmed in 2015 that while not explicitly in the constitution, privacy of the individual and data protection are fundamental rights which derive from other constitutional provisions.

The current primary legislation – the Personal Information Protection Act – was enacted on 30 September 2011 ("PIPA"). It sits alongside other sector specific legislation covering telecoms, data relating to an individual's location and consumer credit. This sectoral legislation is broadly analogous to PIPA.

Currently, there is no one centralised body which is responsible for monitoring, investigation and enforcement; these roles are undertaken by a number of different agencies. This does have broader implications which will be addressed below. The legislative regime, however, is regarded, at least in theory, as one of the strictest in the world.

In general terms, the system is based on the giving of notice and the provision of informed consent following which information can quite freely be transferred. This strict regime has not prevented scandals. In 2014, for example there was a massive leak of personal information by a credit card company.

The law, of course, is relatively new. There has not been that much litigation relatively speaking. Litigation has generally related to the definition of personal information, data breaches, what constitutes informed consent and data sharing.

Sanctions – administrative, criminal and civil – up to this point have not been especially harsh. The corollary effect, however, of data breaches has been to bring these issues – at least temporarily – to the forefront of the public consciousness. The likelihood is that punishment is likely to become more severe.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

The GDPR has had a significant impact on South Korea not least because it is a world leader in ICT with its global companies doing business with the EU, and which see huge commercial benefits in potentially obtaining data from EU citizens.

There are, of course, broad similarities in the impact of technology as it pertains to privacy and data protection in liberal democracies in the EU and in South Korea. Likewise, it is no coincidence that there are broad and significant similarities in the laws of South Korea and the GDPR. There are also significant differences.

One significant difference between the approaches of South Korea and the EU is that in broad terms in South Korea if consent has been given, data can be transferred out of the jurisdiction. The South Korean authorities no longer have any control (or interest) over how that information is used. This contrasts with the approach in the EU and it has produced a legislative response.

South Korea has been seeking an agreement with the EU on the transfer of data since 2015. Initially, this was limited to telecoms. In 2018, the Act for the Promotion of IT Network Use and Information Protection was amended. The law requires digital communications providers which deal with South Korea data but who do not have a physical presence in the country to have a domestic representative to deal with data protection issues.

South Korea is now also looking for broader adequacy approval from the EU. In this regard, the National Assembly is currently considering amending PIPA, in particular by granting enforcement powers to the Personal Information Protection Commission, an agency independent of the government.

As a side note, last year Korea became the fifth member to join the APEC Cross Border Privacy Rules.

Ahnse is a boutique Seoul-based firm which has been providing quality legal services to foreign clients for over 15 years. We have and continue to represent numerous well known multinational companies. Our Senior Partner is also outside counsel to a number of different government departments and NGOs. We advise our clients on both commercial and legal risk; we like to have an understanding of our clients' strategy – when we have a better appreciation of what our clients are trying to achieve, we can provide better advice on business risk.

Data Privacy in South Korea

1. Privacy and data protection are fundamental constitutional rights. The main governing law is the Personal Information Protection Act ("PIPA").
2. PIPA is not comprehensive; there are other sector specific laws covering telecommunications, individual location and personal credit.
3. PIPA and the other laws are broadly analogous. They are based on the provision of notices and the giving of informed consent. Once consent has been given, information can be freely transferred.
4. Monitoring, investigation and enforcement are undertaken by different bodies. Criminal, administrative and civil remedies are available. Sanctions for breaches are likely to become more severe.
5. The South Korean government is currently in negotiations with the EU to enable data to be transferred. Amendments to the law have been enacted and continue to be discussed.

HUNGARY

Jesszika Udvari

Partner, Buzády & Udvari Attorneys at law, Budlegal Hungary

jesszika.udvari@bud-legal.hu
irglobal.com/advisor/dr-jesszika-udvari
+36 23 889 145

Jesszika Udvari has been practising as a Hungarian lawyer for over 15 years. She started her career in the law office operating beside Arthur Andersen and became an independent attorney in 2003. She specialises in real estate law, commercial law, labour law and data protection.

She graduated at the Faculty of Law of ELTE Budapest and afterwards also studied at the Humboldt University in Berlin. Currently, she is an executive MBA candidate at ESMT Berlin.

Ms Udvari is a member of the Hungarian-German Lawyer Association. She is also actively supporting Hungarian non-profit companies as a volunteer lawyer.

Assisting multinational companies in Hungary

Among her various legal activities, she provides consultancy, mainly to small and medium enterprises and international enterprises with an international ownership background. She speaks English and German fluently.

bud-legal.hu/en

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

Every business that holds personal data of an EU citizen is affected and has to deal with GDPR. Not only personal data of clients, business contacts or customers, but also personal data related to employees or contracted parties. And one year after the regulation came into force only a few companies can say they're complying with the regulation.

It is important for businesses to recognise that the compliance with the GDPR is not just that they've updated their privacy policy. To comply, the businesses need to rethink and change a lot of their internal processes and practices.

The regulation imposes less obligations on small and medium-sized enterprises regarding the administration of their data processes, but this rule is often difficult to interpret. Many businesses do not have the appropriate resources to take the necessary regulatory compliance measures or are uncertain if they are bound by the rules of the GDPR.

Technology is an important factor and a big challenge for the next decade in Hungary.

When GDPR was introduced the mandatory electronic online administration in public and judicial proceedings was also in progress. In practice, this meant very often a kind of "duplication" of data processing, which in turn was and still is a significant workload for authorities.

Due to the new rules of the GDPR, there are technologies and systems that can no longer be used or only to a limited extent. Thus, an impact assessment and a well-defined purpose and consideration are needed to determine whether a particular business can use, for example, a fingerprint scanning system to enroll its employees as a fingerprint is biometric data that the GDPR considers as highly sensitive. Similarly, camera surveillance systems using facial recognition software can only be used for the right purpose, to the right extent and by the entitled person.

Most cases before the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter "NAIH") which resulted in warnings or fines were based on an information technology incident. This may be – among other things – the consequence of the fact that access to technology data from clients is usually a challenge for professionals.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

After the GDPR came into force, businesses were given an almost 1-year-long grace period to prepare for the GDPR. As this grace period passed, the NAIH started to impose the compliance regime and the authority has since fined several businesses. Based on our experiences, the NAIH first warns and makes a recommendation when an irregularity is detected, and only imposes a fine after the business has not changed its data protection practices in accordance with the regulation.

Examining the cases, we can see that the authority took into account the degree of public scrutiny of the business and if it could serve as a model for others. Not only does NAIH set examples with fines in the business sector, but it also imposes higher fines in the public sector.

For example, the authority acted against a political party, a local government, a university and the police, clearly establishing the data protection regulations. In one in instance, the authority imposed a fine of 11 million Hungarian Forints (33.000 EUR) on a political party for its failure to report a personal data breach following a cyber attack.

Elsewhere, NAIH is also giving its support for the diverse regulatory environment and recently issued a series of briefings to assist data controllers in their interpretation of the law. For the purpose of a data protection impact assessment in Hungary, the open source software (originally called "PIA software") published by the French Data Protection Authority (CNIL) is recommended by the NAIH.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

In Hungary, besides the GDPR, the Act CXII of 2011 on Informational Self-determination and the Freedom of Information ("Information Act") governs the law of information protection, which has also been amended since the GDPR came into force. The Information Act is comprehensive in scope, as it is applicable to all data processing operations undertaken in Hungary regardless of the public or private legal status of those performing such operations. The Act has been complemented by sector-specific legislation such as the Property Protection Act and the Labour Code containing more detailed rules on data protection.

Due to the new regulation, Hungarian Labour Law has been changed. For the sake of consistency, the Labour Code has been amended, and a new chapter on data protection has been added, containing structured and detailed rules on employee data management.

Elsewhere, the possibility of requesting employee "morale certificates" has been restricted and prohibited, since the employee's personal criminal data may be processed by the employer only for the purpose of examining whether the employment is being restricted or excluded by the law. As an amendment of the GDPR the rules on the use of employees' biometric data have been tightened: biometric data (such as facial image and fingerprints) of employees may be processed by the employer only in cases defined by law.

Indeed, there has been a closer cooperation on data protection between authorities and advisers. We believe that this is primarily due to the need for mutual assistance and the development of a common understanding and practice in the European market on the field of this complex regulation.

Budlegal's clientele mainly consist of international corporations, mostly serving the shareholder level.

We specialise in cross-border M&As, requiring extensive and comprehensive legal and business counselling. Within our transactional work practice, our core areas of law are Corporate finance, Commercial/IPO, Real estate, Labour law and Data protection.

All Budlegal partners work in English and German languages on a daily basis. Budlegal is a member of the German-Hungarian Chamber of Industry and Commerce, and of the Swiss-Hungarian Chamber of Commerce.

Data Privacy in Hungary

1. If businesses from other countries intend to sell products or services to customers on Hungarian territory, they must comply with the provisions of Hungarian data protection law.
2. Hereby it is not enough to update the privacy policy on the webpage or to buy a pack of sample documents. Instead, businesses need to rethink and change their internal processes and practices, and then to prepare compliance documentation, educate their people and appoint an external Data Protection Officer ("DPO").
3. Businesses need to learn and understand their own practices, how data storage and data collection works in their companies.
4. In Hungary, GDPR has had a big impact on marketing practices. Here the data controller needs prior explicit permission of the data subject before sending out any newsletter or marketing material.
5. Commercial and employment contracts shall be amended as to how the personal data will be processed, stored and protected.

SWITZERLAND

Monika Naef

Partner, DUFOUR Advokatur

monika.naef@dufo.ch
irglobal.com/advisor/monika-naef
+41 61 205 03 03

Monika has been a partner with Dufour Advokateur (since 2005). She was previously head of section law of an International Chemicals Group and Legal Advisor to human resources and the pension fund of an International Pharmaceutical and Chemicals Group. She is also a member of the board of several SMEs and spent 14 years living abroad on three continents (USA, Europe and Japan).

Her practice covers employment law (corporate, international, expats), contract, trade and company law, negotiation (management and tactics), mergers & acquisitions (M & A) and dispute resolution (litigation and arbitration).

dufour-advokatur.ch

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

Technological developments are a major challenge. It lies in the nature of law that it reflects social developments after they have evolved. Innovations take place first and only afterwards does the need for regulation arise. This is particularly pronounced in the technology sector where Switzerland is at the forefront of such developments, such as robotics, blockchain technology (ICO's), nanotechnology just to name a few. The rapid advance of technological developments will remain one of the central challenges in the context of data protection.

Enforcement of Data Protection. As more data is generated by various means, the further advancement of mobile devices connecting applications relying on and sharing the same data sources will make it more difficult to control the use thereof and to identify the data processors.

Lack of awareness among data subjects and data processors. The realisation that activities an organisation may qualify as data processing which will require implementation of the necessary protection measures still needs to improve significantly in Switzerland. In addition to the technological challenges, creating awareness both with data processors and those providing their data (data subjects) will also be a central aspect. The awareness of the extent to which data is already being processed, which types of data are being collected and what data subjects disclose about themselves on a daily basis is only just beginning. Data processors bear a considerable risk of being severely sanctioned in the event of a data protection violation. Accordingly, personnel training measures are required and data protection must be integrated into day-to-day business by defining appropriate processes and providing training. In addition, clear rules must be laid down as to who is responsible for data processing.

Cost of compliance. The cost of implementing the necessary measures for compliance in the data protection area will be a challenge for small and medium sized organisations.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

Technology-neutral approach. Swiss data protection law follows a technology-neutral approach, i.e., the statutory data protection provisions are applicable to all types of data processing, regardless of the processing technique. This is to ensure that the law is flexible enough to be applied to future technological developments that are not yet known at the time of enactment. In this way, the legislator also ensures that the protection of personal data can also be enforced in the future.

Increase in sanctions. Under the revised Swiss Data Protection Act, sanctions will become more severe and, as awareness is being raised, data subjects will demand better enforcement. Civil damage claims for breach of data protection will increase. In order to enforce data protection, Swiss data protection

law already provides for draconian penalties for breaches of data protection. In contrast to other legal systems, such as the EU's General Data Protection Regulation (GDPR), it is not the organisation but the individual (natural person) who is liable for any breach of data protection. The sanction concept in Swiss data protection law follows criminal law procedures, which is why the natural person responsible for data processing is primarily liable and can be fined up to CHF 250,000.

The revised Swiss Data Protection Act focuses more on the protection of personal data. In the course of the political debates on the revised law has probably also led to an increase in awareness among data processors and data subjects, and is now punishing breaches of data protection law even more severely than before. This trend will probably continue and be reflected in the final law.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

Model function of the GDPR. Prior to the enactment of GDPR, Switzerland's data protection laws were stringent. But the GDPR is now stricter and as such the EU's basic data protection regulation is a model for Swiss data protection law, which is currently being revised and adapted to European requirements, even though Switzerland is not a member of the EU or the European Economic Area (EEA). Switzerland is currently regarded as having adequate protection from the EU Commission, but without enactment of the revised Data Protection Act this would no longer be the case. Only the adequacy declaration makes cross-border data exchange possible without further assurances, such as special contractual clauses. Barrier-free data exchange with the EU is of central importance for Swiss organisations.

From a Swiss perspective, it is therefore imperative that Switzerland's new data protection law complies with European requirements.

Internationalisation. In connection with these requirements, increased international cooperation between organisations will become necessary. On the one hand, organisations must comply with the data protection standards of each country in which they operate. It is advisable to find a uniform solution for the entire corporate structure, based on the strictest standards. On the other hand, the internationalisation of the standards applicable to data processors makes international cooperation with other data processors and experts both necessary and useful.

Data Privacy in Switzerland

1. Create an understanding that data has an economic value. Ensure that as a data processor, regardless of your financial potential or company size, data protection is treated with the necessary importance.
2. Create awareness in the organisation that data protection is an expression of a fundamental and constitutional right and that with the processing of data comes great responsibility.
3. An organisation must establish data protection as part of its risk management procedures. Accordingly, adequate personnel and technical resources must be deployed.
4. Organisations should consider the benefits of being compliant. Data protection can be a useful marketing tool. Effective and well-functioning data protection procedures can cultivate a positive image.
5. Focus on areas that are most susceptible to breaches of data protection, such as digital processes or the storing of data.

POLAND

Robert Lewandowski

Partner, DLP Dr Lewandowski & Partners

rl@drlewandowski.eu
irglobal.com/advisor/robert-lewandowski
+48 22 10 10 740

Robert is the founder and managing partner of Dr Lewandowski and Partners. He is head of the Warsaw and Wrocław offices. He has previously worked for major legal firms in Warsaw and London and has written many legal books and taught university courses in English, German and Polish.

Robert studied mathematics and German philology at the University of Warsaw, before studying law at the University of Mainz/Germany and passing the second state legal examination in Mainz/Germany in 1998. He enrolled on the list of German attorneys in Frankfurt am Main (2000), then, from 2001 – 2005, he worked as a lawyer at Gleiss Lutz in Warsaw/Poland which included secondment to Herbert Smith in London.

He became an independent lawyer in Warsaw in co-operation with Derra, Meyer & Partners, co-founding the Polish branch of DMP Derra, Meyer & Partners before founding Dr Lewandowski and Partners. During the last 10 years he has overseen the establishment and development of the two Polish offices, while practising and advising clients in his position as the senior figure.

drlewandowski.eu

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

One of the main challenges will be to meet the different requirements of the new Data Protection Regulation (GDPR) and to adapt and, where necessary, renew the existing technology.

In addition, there are various regulations in the GDPR which have shown to be difficult within practical implementation and therefore are also seen as a challenge. For example, Poland has serious concerns about whether certification under Articles 42 and 43 of the GPDR is practicable. The Polish Government considers that the mechanism established in the GDPR does not provide sufficient incentives for data controllers/processors to apply for certification. Accordingly, no certification applications have been submitted so far in Poland.

A further challenge in business life in Poland is the fact that sole proprietorships run by small entrepreneurs are a very popular form of business activity in Poland and these persons are not officially classified as legal persons, whereby the processing of their data also falls under the GDPR. This poses some practical problems for Polish business practice.

Technology is a factor in the sense that GDPR should also reconcile fundamental rights with technical innovation. A new technology that is very challenging in terms of data protection is, for example, the blockchain. Accordingly, European data protection rules should be able to strike a balance between protecting the rights of data subjects and developing new technologies.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

The Europe-wide introduction of the GDPR overshadowed the penalties previously imposed in Poland for violations of the Data Protection Act. Until GDPR, the powers of the Polish supervisory authorities were severely limited. For example, the General Inspector, who was previously responsible for data protection, was only authorised to issue an administrative decision in the case of violations of the Data Protection Act. In such an administrative decision, the company was first reminded to adapt to the requirements of the Polish Data Protection Act.

If the company did not comply with this requirement, the Polish supervisory authority could impose a maximum fine of PLN 50,000 (approx. EUR 11,665.14) or a maximum fine of PLN 200,000 (approx. EUR 46,660.56) on the company in the case of a limited liability company. This year, the Polish Data Protection Supervisory Authority (PUODO) imposed the first two fines on companies for breaching the GDPR. The first fine was imposed on a company that had processed the data of over 6 million people but informed only 90,000 of them about it. The fine amounted to PLN 943,000 (approx. EUR 220,004.55) and was the highest fine ever imposed in Poland for a breach of data protection law. The other fine of PLN 55,000 (about € 12,831.65) was directed against a sports association that failed to delete judicial data. This rigorous approach by the Polish data protection authority shows that an attempt is being made to meet the requirements for the prosecution of data breaches.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

The entry of the GDPR led to the adoption in Poland of a completely new law on the protection of personal data. Among other things, this law includes provisions to introduce the new data protection authority PUODO, which replaced the former Inspector General for Personal Data Protection with the President of the Office for Personal Data Protection. Furthermore, the new law on the protection of personal data contains new criminal sanctions for the obstruction of PUODO investigations as well as regulations for setting the minimum age for the consent of minors to data processing at 13 years. Accordingly, the GDPR has a large influence on the Polish legislation with regard to the data protection regulations.

Moreover, many new issues relating to jurisdiction were intensively discussed. It discusses, among other issues, issues such as profiling, in particular the need for sector-specific exceptions; for example, for banks and insurance companies in order to conduct scoring and anti-fraud or the scope of employee data which could be collected and processed within the employment context.

With regard to the issue of employee data, changes in the Polish Labour Code following the adoption of the GDPR led to significant changes in the work practice and the labour market. One such change is, among other things, the provision of a list of data that must be provided by applicants and workers and that can be requested by employers.

Special data categories can only be processed with the consent of the respective candidate or employee and only if this data was provided on the applicant's or employee's own initiative.

Greater efforts with regard to international cooperation can be seen, for example, in the fact that Poland participated in the submission of a commentary on the current review and evaluation of the DSGVO to the European Council, which was published together with comments from 18 other European member states on 3 October this year.

DR LEWANDOWSKI & PARTNERS
Dr Robert Lewandowski & Partners sp. k.

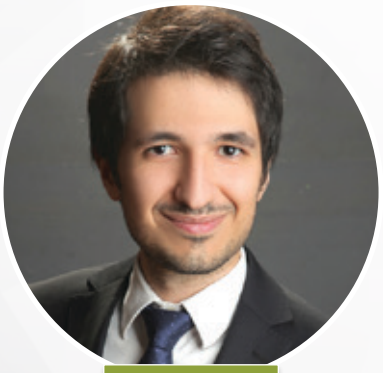
Dr Robert Lewandowski & Partners (former Derra, Meyer R. Lewandowski) has been advising clients for over 15 years in all areas of commercial law. We offer our clients legal services at the highest level.

We specialise in providing legal services to entrepreneurs and private individuals in the business sector. Our main fields of expertise include: M&A, company law, financing, insurance law, real estate law, bankruptcy and restructuring law.

Dr Robert Lewandowski & Partners offers legal advice to domestic and foreign entrepreneurs in local and cross-border cases, based on cooperation with international partner law firms in cooperation.

| Data Privacy in Poland

1. In order to facilitate the data protection process as well as the handling of data protection law, it would be necessary for even more information and advice on data protection to be provided.
2. The setting of transparent and uniform criteria for the imposition of fines would be necessary for comparability and uniform enforcement in the case of data protection offenses.
3. Further guidance is needed on how to prove that a data subject already has the information that otherwise should be provided by a controller, because it is necessary to ensure that the data subjects receive information they need.
4. A good and efficient communication between the Polish data protection authorities and the European Commission and the European Council is necessary for a successful implementation of the data protection process in Poland.
5. An exchange between Poland and the other European member states regarding the difficulties in practical implementation of the data protection regulation.



TURKEY

Yusuf Mansur Özer

Associate, ErsoyBilgehan

yozer@ersoybilgehan.com
irglobal.com/advisor/yusuf-mansur-oezer
+90 212 213 23 00

Yusuf is an associate lawyer at ErsoyBilgehan, mainly focusing on privacy, data protection, e-commerce, telecommunication, and general corporate and commercial law.

He acts for a range of clientele, particularly in connection with data protection and privacy compliance, including employee monitoring, cross-border data transfers, compliance programs, and data retention. His passion for and background in information technologies enable him to not only analyse the matters from a legal perspective but also provide his advice based on technical understanding. He is an active member of the International Association of Privacy Professionals where he previously acted as the Young Privacy Professional Leader for Turkey.

Yusuf holds an LL.M. degree from Bilgi University Information and Technology Law Institute, the subject of his dissertation being 'Blockchain Model in Personal Data Protection: Promises and Legal Challenges.'

ersoybilgehan.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

The biggest challenge for businesses will be to sustain their compliance with the laws and regulations. With the new data protection legislation coming into force in 2016, all businesses rushed to ensure that they are compliant with the law and have built their privacy compliance programs with the help of their consultants. However, privacy and data protection compliance is not a one-time job. It is a continuous process. The key is to create a proactive culture that responds effectively to privacy-related matters. It remains to be seen how and to what extent businesses will be able to incorporate privacy into their day-to-day lives and their mindsets.

Another challenge will be to adapt and revise the privacy programme until it precisely fits with the unique needs and characteristics of the businesses. The compliance programmes designed in meeting rooms and approved by directors will simply not be enough. There will be an abundance of issues when these are applied in the trenches. Businesses will need to be able to respond effectively to these issues and adapt accordingly.

In both of these challenges, technology will have a key role to play. In privacy compliance, technology is usually considered as part of the data security exercise but there is more to it. Technology is a fundamental component of privacy governance. Keeping an up-to-date data processing inventory, responding to data subject access requests, managing vendor and third-party risk, and many others require an efficient process which can only be affected by software and automation. "Privacy-tech", as it is sometimes called, will gain even more momentum as individuals become more informed of their privacy rights and authorities adopt a more aggressive enforcement approach.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

The main regulatory trend in Turkey is that the national supervisory authority is increasingly more aggressive in pursuing breaches and issuing fines. The fines imposed so far range between EUR 10,000 for sending unsolicited messages to EUR 250,000 for data security breaches. According to news reports, the number of pending cases before the authority were up to 800 as of May 2019 and the sum of fines already issued so far had reached EUR 750,000. Since then, the fines imposed and publicised by the authority amount to EUR 1,200,000, a sharp increase of 160% only within 6 months. This illustrates a seismic shift in the authority's aggressiveness in the enforcement of privacy regulations.

There is also an upcoming deadline in relation to the data controllers' registry, which was recently extended from 30 September 2019 to 31 December 2019. Therefore, we expect the authority to be more active in 2020 and focus more on the registration obligations and breach thereof.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

Turkey has been experiencing a data protection hype since the enactment of the Turkish equivalent of the GDPR, Personal Data Protection Law (PDPL), in 2016. PDPL marked a new era for personal data protection in Turkey, as did the GDPR in the European Union. The compliance processes for both of these legislations, therefore, overlapped in 2018, which gave rise to greater efforts at international cooperation.

Businesses that are caught in the territorial scops of the PDPL and the GDPR need to achieve a versatile compliance model that satisfies the expectations of numerous supervisory authorities in diversified jurisdictions. This requires collecting input from consultants from several jurisdictions, but at the same time designing the compliance efforts carefully to avoid any duplication. We have seen compliance projects where PDPL compliance was built on top of GDPR compliance or vice versa. International cooperation was and continues to be key in all these efforts.

ersoybilgehan

ErsoyBilgehan is an independent full-service law firm widely recognised for its strong national and international practice.

Since its foundation in 1999, the firm has acted for enterprises across the full spectrum of business including local, national and multinational companies in a wide range of business sectors. Clients range from single-owner start-ups to household name companies, from government companies to global giants.

ErsoyBilgehan is a law firm which has a strong national presence with a full-scale global reach. It's longstanding network of relationships with pre-eminent law firms around the world ensures it is ready to provide comprehensive legal services in virtually every jurisdiction. In today's fast-changing and inter-connected world, the firm helps its clients thrive in the global economy by drawing on local market knowledge and international capabilities to provide excellent service and creative advice.

Data Privacy in Turkey

1. Methodology. The privacy process should be based on the well-known Deming Cycle. Adapted to privacy compliance, the four phases would be (1) assess, (2) improve, (3) monitor, and (4) respond.
2. Mentality. Compliance projects should not end up aiming for a staccato transition between ground-zero and perfect compliance. The first order of business should be to define a "Minimum Viable Privacy Programme".
3. Business-friendliness. The privacy programme should assess risks and respond accordingly. It should be risk-based and practicable. Stifling the business with hundreds of pages of policies, procedures, and manuals do not help.
4. Adaptation. There is simply no "one-size-fits-all" strategy. Any privacy programme should be constantly adapted and revised until it precisely fits with the unique needs and characteristics of the business.
5. Sustainability. Achieving compliance and sustaining it are completely different things. Privacy awareness should be programmed into the DNA of the business.

Aaron Allan

Partner, Glaser Weil

aallan@glaserweil.com
irglobal.com/advisor/aaron-p-allan
+1 310 282 6279

Aaron P. Allan, a Senior Partner in Glaser Weil's Environmental & Energy Department, has for more than two decades litigated cutting edge and "bet the company" cases for a diverse range of business entities, including significant environmental and insurance coverage cases, toxic tort cases and real property litigation matters.

Mr. Allan has long represented water utilities accused of delivering contaminated drinking water and many other companies subjected to claims brought under CERCLA and other environmental laws.

Alexander J. Suarez

Associate, Glaser Weil

asuarez@glaserweil.com
glaserweil.com/attorneys/alexander-suarez
+1 310 282 6279

Glaser Weil Associate Alexander Suarez specialises in commercial disputes and business litigation. He represents clients in complex commercial litigation involving insurance recovery issues, financial services, and real estate.

Mr. Suarez is experienced in all phases of litigation, from filing and answering complaints, through discovery, trial, and appeals. He has trial experience in both California state and federal courts and also has experience in arbitration.

glaserweil.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

The biggest challenge for data privacy in California will be the implementation of (and compliance with) the California Consumer Privacy Act (CCPA), effective January 1, 2020, which is the most comprehensive consumer privacy protection law in the United States. Like the GDPR, the CCPA has caused considerable uncertainty and concern, particularly given the potential for significant civil penalties, underscoring the importance of compliance. Fortunately, the California Department of Justice recently proposed regulations providing guidance on compliance with the CCPA.

For example, the CCPA obligates subject businesses to notify consumers of the categories of personal information they collect and the reasons for its collection, at or before the time it is collected; it does not say how businesses must satisfy that obligation. The proposed regulations specify that the requisite notice must be in plain language, legible, available in languages that the business uses in transactions with consumers in the ordinary course, accessible to consumers with disabilities, and visible or accessible to consumers before the collection of their personal information. The proposed regulations also provide examples of how businesses can make the disclosure online (e.g., by posting links to the notice on pages where information is collected) and offline (i.e., by giving notice on forms and via conspicuous signage). Businesses wondering what they must do to comply with the CCPA should consult with legal counsel or look to the implementing regulations for more specific guidance.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

California has shifted toward consumer empowerment in data privacy enforcement. The legislative history of the CCPA shows the Legislature recognised the enormous value of consumer data, and drafted the act with the express purpose of giving consumers greater control over their personal information. The Senate Judiciary Committee's August 31, 2018 Bill Analysis observes: "The world's most valuable resource is no longer oil, but data" and "[w]ith [the] widespread collection of data comes serious concerns about consumers' privacy." The Analysis affirms that the CCPA's "goal was to empower consumers to find out what information businesses were collecting on them and give them the choice to tell businesses to stop selling their personal information" and to provide "a modified enforcement mechanism to protect those rights."

Even in the absence of a data breach, the CCPA empowers a consumer to request that a business subject to the act:

- disclose the categories and specific pieces of personal information about the consumer collected or sold;
- delete personal information that the business collected from the consumer;
- disclose types of personal information about the consumer sold to third parties, and describe the categories of third parties to whom the information was sold; and

- not sell the consumer's personal information to third parties.

The CCPA is primarily enforced by the Attorney General but it also provides for a limited private right of action for consumers whose "nonencrypted or nonredacted personal information" is subject to "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures."

If the consumer gives the company written notice specifying which provisions of the CCPA it violated and if those violations are not cured within 30 days, the consumer may sue, on an individual or class-wide basis, for statutory damages of between $100-750 per consumer, per incident or for actual damages, whichever is greater.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

On September 24, 2019, the European Court of Justice ("ECJ") decided Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), and in the process construed Article 17 of the GDPR. Article 17 allows individuals in European Union Member States to request that their personal data be erased in certain circumstances, for example, where the person objects to the processing of his or her personal data on certain grounds and the data controller does not demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims." This has also been referred to as the "right to be forgotten."

In Google LLC, the CNIL demanded, in response to a request for erasure under Article 17, that Google remove information subject to the request globally, and not just from results for searches conducted within EU Member States. Google refused, removing the information subject to a request for erasure only from results for searches conducted within EU Member States. The ECJ's preliminary decision was in favour of Google's interpretation of the right to be forgotten. As a result, Google can make information subject to a GDPR request for erasure available outside of EU Member States.

The decision calls into question whether the GDPR will drive greater efforts at international cooperation in data privacy and information security. The ECJ's ruling was very important to tech firms in Silicon Valley, particularly internet search providers and social media companies. The ruling makes clear that the right of erasure requires only that the information subject to a GDPR request for erasure be made inaccessible in EU Member States, but may nevertheless be made accessible in non-member states. It is worth noting, however, that the CCPA mirrors many of the GDPR's consumer protections, exceeding them in certain respects.

Data Privacy in California

1. Get ready for California Consumer Privacy Act (CCPA) compliance. On January 1, 2020, consumers will have the right to request personal information about them collected or sold by a business during the preceding 12 months.
2. Ensure ongoing compliance with federal, state, or local laws governing data privacy. These laws are not impacted by the CCPA.
3. Keep current with cyber-insurance coverage. Given the potentially devastating costs of a data breach, businesses must keep current with the rapidly evolving landscape of cyber-insurance coverage.
4. Develop a data breach response plan and practice its implementation. An actual data breach should not be the first test of your response plan.
5. Take a multi-jurisdictional approach to data privacy compliance. For example, compliance in California may not satisfy obligations under the EU's General Data Protection Regulation (GDPR).

SPAIN

Sönke Lund

Partner, Grupo Gispert

sonke.lund@grupogispert.com
grupogispert.com/en/team/soenke-lund
+34 934 594 071

Sönke is partner responsible for the departments of competition law and commerce, intellectual and industrial property law, as well as economic international law at Grupo Gispert. He has more than 20 years of experience advising companies from the national and the international market.

Sönke was previously a partner of a leading law firm in the German-Spanish market where he led the practice of Intellectual and Industrial Property, Competition and Information Technologies. He is Rechtsanwalt (German lawyer), graduated and member of the Bar Association of Hamburg and lawyer of the Barcelona's Bar Association.

He is listed in Chambers Global and Best Lawyers as a leading lawyer in Intellectual Property in Spain and Germany, and in Who is Who Legal as prominent expert in Franchise Law.

grupogispert.com/en

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

The challenges for data privacy will come from different directions and will certainly have a close relationship with technology. Generally the biggest challenges will be in the following areas:

a. Anonymisation and pseudonymisation in the context of blockchain.

   Under the GDPR, personal data processed through blockchain raises the important question of whether market participants should be characterised as "data processors" or "data controllers", which will be the key threshold issue to determine the scope of their legal obligations and liabilities. Blockchain's decentralised architecture and the B2B cooperative approach will complicate this determination.

b. Data ownership and data access.

   Regarding data ownership and data access, different questions arise:

- How data can be protected from an IP and civil law perspective?
- How does the international use of data and protection of data match with unfair competition law?
- When should data be considered non-personal and which claims do individuals have affecting the data asset?
- And finally, which rights exist for companies to get access to data under antitrust law?

All these questions are relevant, but the basic question will lie in competition law, where two main questions have to be solved:

- Can there be any right of access to data from an antitrust point of view?
- Insofar as such access is to be granted, how is this access relationship still to be specifically designed?

In principle, data access can be subject to the strict requirements of compulsory licensing claims under antitrust law. But their exact design in practice still depends on many specific questions such as the structure of access, whether through handover, enabling read access or even provision via a dedicated standardized interface, etc.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

The following are the most significant enforcement issues which have arisen in Spain:

The Agencia Española de Protección de Datos (DPA) has carried out numerous proceedings related to the disclosure of data to solvency and credit agencies and to unlawful contracting and unsolicited marketing. It's worth noting that there have been an increasing number of prosecutions carried out and sanctions imposed by the DPA against non-Spanish and non-EU controllers. In fact, the DPA is participating in coordinated activities with other EU authorities to investigate companies that are based in the US but carry out processing activities in the EU.

Moreover, the Constitutional Court recently made a decision broadening the scope on the right to be forgotten. According to the ruling, the right to be forgotten refers to the obligation of a search engine to remove relevant links and the duty of relevant media that published the information to remove the personal information from its internal site's search engines.

Interestingly, regarding initiating class actions under GDPR, a new framework has been created giving rise to news regarding the potential initiation by the Spanish consumers association of class actions related to data protection infringements.

Summary on other trends:

A new privacy law developing some aspects from GDPR was passed in December 2018.

There have been only a few sanctions awarded since GDPR became enforceable. As for now, the DPA has focused more on assessing infringements and sending out warnings to companies. It's worth mentioning a fine of 250,000 euros against "LaLiga" (the men's top professional football division of the Spanish football league system) for infringing the principle of transparency enshrined in the data protection legislation.

Additionally, the DPA fined Vueling Airlines €30,000 for failing to provide a compliant cookies disclosure under GDPR.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

Although the pre-existing data protection regulations have not been formally repealed, GDPR's regime on international transfers is the only regime that applies to transfers in Spain. But, along with the GDPR, there are legal requirements that could be understood as 'restrictive measures' (tax regulations on invoicing obligations, gambling regulations and other specific public administration regulations), so other rules may apply in the affected areas.

In terms of efforts at international cooperation, even beyond the EU borders, there are several points worth mentioning.

Firstly, the principles of jurisdiction, applicability and enforcement where more than ever:

- sovereign borders versus borderless Internet pose problems for determining jurisdiction;
- technology convergence occurs in sectors that used to be separate and distinct;
- regulators struggle to force new multidisciplinary industries into existing structures in terms of data protection.

Furthermore, it is matter of fact (and time) that data protection may be held responsible for the creation of (new) barriers to trade. But not only data flows and data protection regulatory issues will be getting more relevant here. Offering goods and services to EU citizens and online tracking addressed to the EU or Spanish market may trigger the application of the data protection provisions of the GDPR and the Information Society Services Act, cybersecurity as well as the consumer regulations, irrespective of where the organisation is established.

Founded in 1940, Grupo Gispert provides legal advice both at national and international level, to business and individuals from its offices in Barcelona and Madrid.

To understand the global needs of the client beyond the hired service, the firm has set up a multidisciplinary team of highly qualified lawyers and economists that design the best strategies to help clients to reach their goals. The team comprises more than 35 professionals with a target of excellence of service for clients.

At Grupo Gispert we believe that every client is a new challenge to prove our value and earn our trust. We also believe that progressing together and advising the client in all phases of its business makes us a better firm. We know that these goals may be achieved only with the effort and commitment of every member of our team.

Data Privacy in Spain

1. Check if a Data Protection Officer (DPO) is needed. The company should designate someone to assume data protection compliance responsibilities and assess where they will be located in the organisation's structure and governance arrangements.
2. Draft and update the list of personal data processing activities. It's important to understand the legitimate grounds for the data processing activity under GDPR, which should be documented and updated in the privacy notice.
3. Gap analysis. Ensure that you have in place the correct processes to detect, report and investigate any personal data breaches.
4. Security of data. Technical and organisational measures – TOMs – must be implemented to ensure the security of personal data processed in the company. This measure follows the principle of "integrity and confidentiality", which underpins the GDPR.
5. Document support. Contracts will have to be adapted to data protection laws. The corresponding notices on the company's website will have to be revised.

SWEDEN

Anna Fernqvist Svensson

Partner, hellström advokatbyrå kb

anna.fernqvist@hellstromlaw.com
irglobal.com/advisor/anna-fernqvist-svensson
+46 8 22 09 00

Anna Fernqvist Svensson is a partner of Hellström Law. Her areas of practice are Data Protection Law, EU/Competition Law and Corporate & Commercial Law. Since the Swedish Personal Data Act of 1998, she has assisted clients to resolve their legal issues including work with audits, drafting of agreements and policies. She is currently assisting clients with their internal work to become compliant with the GDPR.

Anna is a member of the Swedish Bar Association and of the Swedish Academy of Board Directors (certified director), the ICC Digital Economy Committee; the ICC Competition Committee, Network leader of the JUC Network on Personal Data and Privacy, DP Forum (data protection), SIJU (Swedish Organisation for IT & Law), President of the Election Committee of the French Chamber of Commerce, President of Club Södermark (not-for-profit organisation participating in the Nordic Competition on the Human Rights) and the Swedish Forum for Competition Lawyers. She is also a very experienced lecturer.

Anna holds an LL.M. degree in EC Business Law from the Amsterdam School of International Relations (A.S.I.R.), the Netherlands.

She speaks Swedish, English, French, German and Italian.

hellstromlaw.com/en

QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

Increased digitalisation in Sweden makes Swedish public and private players more vulnerable and they therefore must protect themselves. There have been failures at several public authorities and other organisations regarding data breaches and the level of security is often inadequate. The Swedish Security Service (Sw. Säkerhetspolisen – SÄPO) has previously said that this is one of the biggest security challenges facing Sweden today. When security levels are not keeping up with digitalisation, the threat against these organisations is increasing and thereby also the threat against the protection of personal data. Technology is a big factor. Security knowledge has to increase and better technology has to be installed to prevent attacks.

Another issue is the unique Swedish system with the possibility for database providers to get a so called publisher's license (Sw. utgivningsbevis). With such a publisher's license the database becomes protected under the Swedish constitution. Such databases are exempt from the scope of the GDPR, with reference to the freedom of speech. The publisher's license is granted provided that certain basic requirements are fulfilled, such as the database being available for the public, that it can only be altered by editorial staff, and that the name of the database does not contain a domain name. However, there are no requirements posed concerning the content or purpose of the database/organisation applying.

Another challenge is the management of emails under the GDPR. The previous Swedish Personal Data Act (1998:204) stipulated an exemption for personal data processed in unstructured form, such as in running text – in an e-mail or on a web page. Such personal data could be processed, provided that the data subject's personal integrity was not violated. This exception is known as the "misuse rule" and was used by the majority of the Swedish data controllers with regard to data processing in e-mails and on web pages. I believe that establishing GDPR compliant routines with regard to e-mails is a big challenge in Sweden.

QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

The Swedish data protection authority Datainspektionen is active in its supervision. The first national integrity report issued by Datainspektionen a year after the enforcement of the GDPR showed that three out of four Swedes were worried about how their personal data was handled. The report also stated that the majority of the citizens were aware of the GDPR and of the fact that the regulation enhanced the individual's rights. In connection to launching the report, Datainspektionen stated that "the citizens must be able to feel digitally secure, in order for Sweden's ambitions with regards to digitalization shall be successful".

The first fine for violations of the GDPR was issued in August 2019, obliging the high school board of Skellefteå to pay SEK 200 000. The school in Skellefteå had, as part of a pilot programme, used facial recognition technology in order to track student attendance. Datainspektionen stated that the consents collected had not been valid, and that the use of facial recognition technology was not necessary to fulfil the school's need to document the attendance of the students. When deciding upon the fine, Datainspektionen took into consideration that the processing of personal data had been limited to a period of three weeks, and that only 22 students had been affected.

Sweden has a tradition of issuing low fines, but I believe this will be subject to change during the coming years. We can also expect more fines to be issued as Datainspektionen is continuously active in its supervision.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

The GDPR has had great impact to ensure that individuals as well as companies paying attention to and be aware of the data privacy legislation in general. The GDPR has also had great impact on the public sector in Sweden.

As previously mentioned, a report from the Swedish data protection authority shows that the majority of the Swedish citizens are aware of the existence of the GDPR and of the fact that the regulation enhances the individual's rights.

We are definitely seeing greater efforts at international cooperation, in the Nordics as well as on a European level.

The Nordic data protection authorities of Denmark, the Faeroe Islands, Finland, Iceland, Norway, Sweden and Åland met in the beginning of May 2019 for the annual Nordic Data Protection Meeting. These meetings are a forum for the Nordic DPA's to discuss data protection matters as a part of a close Nordic cooperation. This year, the discussions were especially focused on joint enforcement strategies and EU cooperation, as well as information sharing. It was agreed that the Nordic DPA's will continue contributing to the work of the European Data Protection Board (the "EDPB") and the importance of a close cooperation within the EDPB was emphasised. This is one example of Sweden and the Nordics raising the potential successes brought by international cooperation.

Datainspektionen has also been appointed to lead two working groups within the EDPB. One of these working groups has been established with the purpose of issuing new guidelines regarding the interpretation of the concepts "data controller" and "data processor", as well as the obligations connected to each concept. The other working group, led by the Swedish, British and Dutch data protection authorities, has been assigned to work towards harmonising the fines issued for violations of the GDPR, by creating a uniform assessment of the size of the fine for violations of the same character.

ENGLAND

Matthew Lea

Senior Solicitor, Herrington Carmichael

matthew.lea@herrington-carmichael.com
herrington-carmichael.com/our-people/matthew-lea
+44 118 989 8155

Working in the Corporate and Commercial department since 2012, Matt predominantly acts for clients with corporate legal requirements.

With a specialism in data protection and privacy law and as a certified member of the International Association of Privacy Professionals, Matt is able to advise clients on complex data protection and GDPR matters as well as wider corporate matters.

herrington-carmichael.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

Uncertainty provided by Brexit extends to data protection. At the time of writing, the provisions of the GDPR are still in force. This position, however, may be liable to change as a consequence of Brexit.

While unconfirmed, the UK government has announced that it intends to adopt the provisions of the GDPR into domestic law following Brexit.

Further to the requirement for UK companies to comply with the future provisions of domestic law, the data protection position with the EU will also pose a significant challenge. This is because, if Brexit occurs, the UK will, as things currently stand, be deemed a third country for the purposes of data protection, which will require the implantation of safeguards or application of a derogation when UK and EU companies wish to transfer data to each other. This most practical solution for the majority of UK and EU businesses will be to enter into Standard Contractual Clauses, although this has the potential to cause delays for businesses as they rush to enter into these before communications between the UK and EU continue.

As this will be a new position for entities based in the UK, there will be a challenge in the months and years following Brexit to ensure that compliance is achieved both on the domestic front, the EEA front and an extra-EEA front, heightening the regulatory burden on these entities. Many of our UK clients with an international element to their business have already started preparing as best they can for this, but the uncertainty surrounding Brexit and the data protection landscape post Brexit certainly isn't helping.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

Since GDPR came into full force on 25 May 2018, the attitude towards data protection and individual's rights to privacy in the UK has shifted dramatically. With the EU-wide attention the new legislation gave to privacy laws, many individuals and businesses that hadn't given it a second thought in the past, now have a fresh concept of data protection at the forefront of their minds.

There have been many high profile breaches and investigations in the UK, with the UK's regulator, the Information Commissioner's Office (ICO), handling almost 6,500 cases relating to data protection in the past 12 months and issuing notices of intention to fine where appropriate. The two stand out notices were received by Marriott International (£100m) and British Airways (£183m).

The implementation of GDPR with its strengthened requirements for organisations to report personal data breaches has resulted in a significant increase in reports received by the ICO; up to 13,840 in 18/19 compared to 3,311 in the year before. Complaints sent to the ICO also rose steeply with 41,661 complaints being received in 18/19 against 21,019 being received in 17/18.

The ICO has a clear strategy for keeping up with the increasing regulatory requirements; it has hired more case handlers with staff growing to 700 from 505, improved the ways in which it resolves cases enabling it to close two-thirds of cases within 30 days, and the creation of a new executive committee with a remit for technology strategy to ensure the ICO can maintain its reputation as being at the forefront of data protection regulators.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

Considering the scope of the potential penalties under the GDPR, many companies took swift action to ensure compliance with its provisions. The data protection landscape has unrecognisably changed with many of our clients now reserving a space on their board meeting agendas for data protection and compliance. Not only are companies weary of the potential fines under GDPR, they are also now aware of the significant damage that can be done to brand and reputation for breach of data protection laws, especially those companies that provide software or technology which is heavily reliant on personal data.

Swathes of consultants advertising GDPR and data protection compliance skills began to pop up in the year leading up to 25 May 2018, the implementation of GDPR created a mini industry of its own.

On all of our deals, whether domestic, international or where inward investment is being made into a UK business, we have seen increased attention being paid to whether or not the target is compliant with GDPR. Often, where the target has compliance shortcomings, we will find that investment will not be made unless improvement is made as the investors do not want to risk their money being used to satisfy a fine. Many transactions will also now include extensive data protection due diligence, warranties and where there is particular concern, indemnities. However, some practitioners try to use GDPR as an excuse for inclusion of indemnities, which should always be resisted.

The extra-territorial scope of the GDPR has certainly increased international co-operation when it comes to data protection with the principles being recognised by many of our non-EU clients and network.

One area to watch on the international stage in the future will be the interplay between the Western world's attitude to data protection compared to that of countries where data protection is a foreign concept and the impact this may have on the Western world's ability to keep up with technological advances in fields such as Artificial Intelligence.

Herrington Carmichael
SOLICITORS

Herrington Carmichael LLP is a leading commercial law firm based in the United Kingdom; its clients ranging from individuals to international businesses; offering advice on corporate and banking services, property and real estate matters, tax and estate planning, employment law and dispute resolution/litigation.

Herrington Carmichael LLP aims to establish and build long-term relationships with its clients, taking the time to understand their business, long-term objectives and concerns.

With experience of working with clients looking to invest or expand into the United Kingdom, the firm offers high-quality and commercially astute advice to both private individuals and businesses alike. The Corporate and Commercial Team is highly experienced, working with clients across a range of industry sectors.

Data Privacy in England

1. Be proactive. Discuss data compliance with a specialist before starting a project – it is harder to unpick at the end than it is to plan at the start.
2. Be positive. Data compliance doesn't have to be daunting; it can be a positive for your business and customer – it simply requires a strategy to ensure you can use the data how you want to.
3. Embed compliance. Intertwine compliance procedures with the everyday operations of the company so it becomes second nature.
4. Record decisions. Be able to demonstrate why a certain decision regarding personal data was made, this will help with any future investigations.
5. Practice. Like a fire alarm drill, your organisation should be ready to respond automatically to any issues rather than panicking when one arises and making the wrong decisions.

DENMARK

Henrik Christian Strand

Associate Partner, Holst, Advokater

hcs@holst-law.com
irglobal.com/advisor/henrik-christian-strand
+45 8934 1144

Henrik Christian Strand provides commercial and legal advisory services to housing associations, banks, insurance companies and commercial lessors.

Henrik specialises in data protection, employment law, bankruptcy and debt collection. Henrik also has extensive litigation experience, including cases before both the Danish High Courts and he has been admitted to practice before the Danish Supreme Court.

Henrik's advice is typically aimed at commercial undertakings in Denmark and abroad. Henrik is a certified arbitrator and member of the Danish Arbitration Association.

holst-law.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

The introduction of the GDPR in the EU was the kick-off for a new global personal data movement. Inspired by the principles of the GDPR, an increasing number of countries are considering, discussing, introducing and implementing data protection rules. For many companies, the requirements for processing personal data have dramatically changed the way and purpose of how data is processed. Nowadays, companies store large quantities of backups on personal data – both ordinary, sensitive and vulnerable data. Due to the considerable risk of this information being compromised, significant fines have been introduced, if such information is stored without a lawful basis. In future, companies must consider which data to store.

Another focus area is the rapidly growing blockchain concept. Unlike many other technologies, blockchain is not hosted on a single or few computers, but on many thousands of computers. The system is self-controlling and encrypts data to such an extent that it is almost impossible to change, as the data is not stored in one single place. On the one hand, data based on blockchain is very secure, but on the other hand, data is available to many. Each block in the chain contains a cryptographic reference to the previous block – a timestamp making it very difficult to change former transactions. The difficulty of changing former links in the chain is likely to present a number of challenges in relation to the GDPR provision on the right to be forgotten. The challenge is that blockchains which are "contaminated" with personal data are difficult to replace, anonymise or erase. Thus, in the further development of blockchain technology, it is important to integrate "privacy by design" into the technology in order not to risk developing a system where the entire chain and thereby its value becomes worthless if personal data is to be erased.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

One of the most controversial issues related to the introduction of GDPR in 2018 was the significant administrative fines, which a supervisory authority could impose in the event of non-compliance with the regulation. It is Danish public law that fines characterised by being a criminal sanction can only be imposed by the courts of law. Hence, the Danish legal system does not allow the Danish DPA to determine administrative fines as set out in the GDPR. Therefore, article 83 (9) of GDPR provides for an exception to the general rule of administrative fines, from which it is set out that where the legal system of the Member State does not provide for administrative fines, fines shall be imposed by competent national courts. In order to comply with the provisions of GDPR, Denmark has introduced a system where the DPA initiates the fines, which are then imposed by the national courts.

It was the intention of the EU that when developing the Danish system it should be ensured that the level of fines were equivalent to that of the other EU countries; this is, however, complicated by the fact that the fines are ultimately determined by the courts and not by a supervisory authority. So far, the DPA has recommended fines for two companies for breaching the GDPR. The first fine was in March 2019, when a taxi company was was told to pay a penalty of approximately EUR 160,000 for only erasing the customer's name after a two-year storage period – but not the customer's phone number. Information about the customer's taxi rides (including pick-up and drop-off addresses) therefore still referred to a physical person through the telephone number, which was not erased until after five years. The second fine was in June 2019, when a furniture company was fined approximately EUR 200,000 in consequence of the company's failure to erase name, address, telephone number, e-mail and purchase history of 385,000 customers in their IT systems, and company did not either have any deadlines for erasure of said personal data.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

With the introduction of GDPR, all companies in the EU were affected by the new requirements, whose primary purpose was to intensify and standardise data protection for individuals in the EU. The regulation will ensure citizens in the EU control their personal data and simplify legislation pertaining to international trade by standardising laws and regulations in the EU. This means that all companies – regardless of location – that collect data, sell goods or services to individuals residing in the EU shall abide by the rules. GDPR therefore contains a number of specific rules for the transfer of personal data to so-called third countries, which are also known from the data security directive. It should be considered whether the transfer is made to secure or non-secure third countries. So far, the EU Commission has classified Andorra, Argentina, Switzerland, the Isle of Man, Guernsey, Jersey, Israel, New Zealand, the Faroe Islands, Uruguay and Japan as secure third countries. Certain areas/sectors in Australia, the US and Canada have also been classified as secure. It is our opinion that the possibility of outsourcing, e.g. IT services at which processing of personal data takes place, will be affected by whether the receiving company is operating from a secure third country. Companies operating in secure third countries will have a competitive advantage in the European market, since the mutual recognition will simplify the provisions and documentation required for transfer between the EU and such countries, even though EU based organisations must still ensure that necessary data processing agreements are concluded with the receivers in the secure third countries. This way, a number of administrative burdens are avoided in respect to companies operating in non-secure third countries.

Holst, Advokater

Holst, Advokater was established in 2007 and is a large commercially focused law firm headquartered in Aarhus and has office facilities in Copenhagen too. A total of 90 people work with Holst.

We provide full-range advisory services to commercial clients in Denmark and abroad, to the public sector and to private clients under the highest professional and ethical standards based on our corporate culture and core values to cater for our clients' needs for flexible advice and sparring.

Holst supplies value-adding solutions in close cooperation between our clients and skilled employees.

Our clients' success is our success.

Data Privacy in Denmark

1. If all countries in the world were to abide by the GDPR, there would be no concern about the country where the data is being transferred to and from.
2. If private emails as a main rule could be sent securely in order to ease communication with data subjects.
3. If data subjects became more aware about "contaminating" companies with unnecessary personal data.
4. If IT became more transparent for companies in order for companies to gain more knowledge of their own personal data processing.
5. If more companies were more adaptable to an increased digitalisation.

ROMANIA

Adelina Dospinescu

Managing Associate, Hristescu & Partners

adelina.dospinescu@hmpartners.ro

hmpartners.ro/crew

+40 736 600 304

Adelina Dospinescu has a wealth of experience in various areas of practice: banking support area, finance, civil/commercial, IT&C, IP law matters, data privacy.

For 5 years she was a member of the local corporate counsel team of a global banking group where she coordinated the team for a significant period of time. As an expert she was delegated local data protection officer.

As Senior Associate within a first-tier law firm she coordinated for one year the due diligence analysis and advice on several local foreign investments in real estate projects. Previously, for almost 4 years, she was litigator in the central public administration in a significant number of cases on the Romanian (formerly) Supreme Court of Justice.

She graduated the Faculty of Law of the University of Bucharest and has a Master Degree in Public Policies at the University of Bucharest.

hmpartners.ro

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

Technology will certainly be a game changer on the local level. Innovative business models such as FinTech (in the context of the EU FinTech ActionPlan) could be one of the biggest challenges for the next decade.

There is no doubt GDPR will be a challenge and will remain as such for a while. But this challenge could be even bigger because of the legal requirements for the "open banking eco-system" (together with the Payment Services Directive) and for the free movement of data within the EU, to sustain the single market's FinTech strategies.

In this plan as well as in similar ones, data privacy will have a significant role to spotlight compliance in this domain for each industry. Under the umbrella of GDPR and of the e-privacy acts, the protection level will depend locally on precise and effective elements such as technology and security of the technical systems, cybersecure infrastructure, well trained employees and more transparency ensured towards data subjects.

Romania has already signed the May 2019 OECD Recommendation on Artificial Intelligence ("AI"). Thus, in future, implementing the observance of the "Human centred values and fairness" principle, which includes privacy and data protection through the AI lifecycle, may become another local challenge – for the relevant technology industry and specific legal environment.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

From the national supervisory authority's recent announcements and its 2018 publicly available report, the GDPR compliance process is possible to play a significant role for the companies. This will include administrative sanctions, fines, complaints of data subjects.

Taking into consideration the extended powers of the supervisory authority granted by the local law on the exercising controls or handling complaints, we do envisage an increase in the number of cases involving data subjects and data privacy, providing for claiming potential damages.

We also expect to see a lot more commitment by organisations eager to ensure compliance with GDPR such as dedicated communication channels for the data subjects' rights (via the controllers), security certified technical applications and guarantees for DPOs to play a more effective role to adhere to the respective industry's relevant code of conduct.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

Prior to GDPR, there was local legislation and a national public register of controllers, and the supervisory authority's website hosted most of the relevant acts and information in privacy data in Romania. Nevertheless, there were only a few experts with a dedicated area of practice and most of data privacy practice was in the banking, insurance and telecommunications sectors.

Since GDPR, in Romania data privacy has gained far more attention and data privacy compliance plays a big role in private and public organisations.

From an international perspective, at the business level applying GDPR has faced some unexpected issues, especially regarding companies from third countries. Whenever adequacy decisions are adopted, publishing them on the European Commission's website helps, but it is still not enough. I believe that a centralised chart for the exceptions, limits, or other relevant information would be a great help, particularly if presented in a simple format.

Binding Corporate Rules is another example where it might be difficult to provide a response for an appropriate safeguard in a timely manner to fit with business expectations.

In brief, for the local business relationships with entities from third countries, sometimes the data privacy formalities last longer than the business activity itself.

It's my view that a more recognisable international protection of data privacy law would help, particularly with innovative business models, ie using AI.

Hristescu & Partners
Societate Civilă de Avocați

Hristescu & Partners is a law firm that provides legal services for Romanian and international companies, including assistance and representation, with strong credentials in business law.

Indeed, the language we use is "business", as we are also entrepreneurs and deal with an ever changing and challenging business environment. It is our empathy and experience that gives us the power to understand business and share advice that goes beyond mere legal expertise.

Personal liaisons and common values matter most to us, both in life and in business, so we cultivate new customers and we look carefully at the long-term. When we connect, we become part of a business.

Data Privacy in Romania

It is relevant to clearly explain the importance of data privacy, ie it is a matter of the individual's rights and freedoms and of control of her/his data. At this point the process becomes clearer for clients. It helps to mention that GDPR represents a part of the overall legal framework for the individual's data privacy rights. Along with e-privacy, it's worth highlighting real cases, public debates and court decisions as a way to enhance people's understanding the importance of the processes involved.

Using a specific methodology for assessments, preparing customised documentation, in-depth discussions and training on practical aspects, we give our clients a clearer approach of the policies and processes, of controls and their roles in data privacy.

Lavinia Junqueira

Partner, Junqueira Advogados

lavinia@jlegalteam.com
irglobal.com/advisor/lavinia-junqueira
+55 119 7205 4368

Lavinia has more than 20 years of experience as a lawyer, advising financial institutions and companies, while structuring and implementing financial transactions in Brazil and abroad, including regulatory and tax issues.

She acts as senior counsel to Brazilian multinational companies, and has extensive experience with legal issues related to the Brazilian financial market, including the Brazilian Central Bank foreign exchange regulations, tax and regulatory advice for financial institutions, and assistance to international banks to structure and set up their Brazilian operations.

Cauê Rodrigues Amaral

Associate, Junqueira Advogados

caue@jlegalteam.com
+55 119 7205 4368

Cauê worked in renowned law firms in São Paulo, international banks and multinational companies as a tax consultant, advising financial institutions and companies, while structuring and implementing financial transactions in Brazil and abroad, including regulatory, accounting and tax issues.

He has a solid ground expertise on tax matters related to the Brazilian and international capital markets, such as financial institutions, asset managers and placement agents.

jlegalteam.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

In today´s digital world, increased reliance on cyber infrastructure comes with increased risk, especially in Brazil, which sits at 2nd in the Global Cybercrime Ranking. The so-called “detection and response” solutions are currently one of the most efficient information security projects to mitigate data leakage and theft risks. I believe the big challenge for the next 10 years is to develop advanced analytics capabilities that can detect sophisticated fraud and cyber-attacks much more quickly and efficiently. And this is only possible through technology.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

In light of the recent publication of Law No. 13,709/18 in Brazil (“Brazilian General Data Protection Law” or “LGDP”), which will become effective on 16 February 2020, the LGPD establishes detailed rules for the collection, use, processing and storage of personal data in Brazil. This statute is applicable to private and public entities in all economic sectors, both in the digital and physical environment.

Considering a rapidly changing regulatory environment in Brazil, data privacy has become an even more critical point for organisations and has been reinforced by the adoption of new standards that often end up drastically affecting their business strategy, purpose and methods for processing personal data. Violations of the new standards set by LGDP may have financial, reputational and regulatory implications for organizations.

Consequently, many measures have been taken by institutions, such as implementing an effective compliance programme, hiring information technology resources and training staff to comply with the rights of data subjects and to avoid sanctions and fines set forth by LGDP.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

2018 has been a watershed year for the privacy field. The GDPR has been the main attraction. The GDPR had an immediate impact in Brazil and there is no doubt that LGPD was significantly inspired by the GDPR rules.

Due to the trade relations with the members of the European Union, Brazilian companies operating in the international market have expended enormous efforts and funds to understand and document their data-processing operations, which will make them fit LGDP more easily.

Following the GDPR model, LGPD has created a modern regulatory framework, including ensuring Brazil is in the list of countries and international organizations able to provide a degree of personal data protection deemed adequate by international standards.

The firm is structured to provide specialised legal services for players in the capital markets as well as wealth management industries, building true connection and real relationships with clients by overcoming the challenges presented on the daily basis.

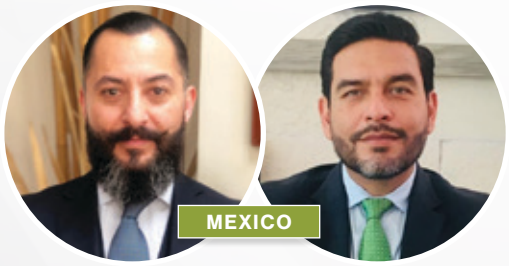
It constantly works in partnership with corresponding offices throughout the national territory and internationally, foreign banks and professionals from other areas of expertise aiming at a multidisciplinary work, especially in the corporate, finance and accounting areas.

This dynamic operation allows the firm to deliver tailor-made solutions to their clients, thereby enhancing the understanding of their business and making them valuable partners.

The firm is also noted for its solid experience in tax and regulatory issues related to financial markets, structuring private equity and venture capital transactions, advising on foreign exchange regulation, structured transactions and capital markets regulation and representing local and foreign mutual funds, asset managers, institutional investors and individuals.

Data Privacy in Brazil

Organisations need to review client intake to deal with data gathering and sharing, need to identify what they know about clients, where information is stored, how it is accessed, shared. They need to review cybersecurity issues, build complete workflows, allowing companies to make innovative uses of data, to protect them, to be accountable to the individuals to whom the data pertains and to be responsive to occasional breaches, implementing fallback plans, communication plans and insurance coverage. While building workflows and practices it is key to benchmark and collaborate with other companies to share understanding and expertise to facilitate this process because doing so can expose the company to greater resources and expertise that can help to better protect customers' data. Create internal data protection communication channels, appoint a Data Protection Officer (DPO) and continuously monitor access to data and change in regulations.



Oscar Conde

Managing Partner, Legem Attorneys at Law

oconde@legem.mx
irglobal.com/advisor/oscar-conde-medina
+52 81 8143 0700

Legem Attorneys at Law, SC. was founded in 2006 to support foreign direct investment in Mexico. Founder and Managing Partner Oscar Conde Medina has more than 20 years of experience dedicated to attracting, consulting and assisting direct foreign investment in Mexico. In 1996, he supported and participated, together with other experts, in the purchase of one of the most important financial institutions in Mexico, which was Banca Confia, acquired by Citibank.

Dr. Juan José Rico Urbiola

Counseling/Compliance, Legem Attorneys at Law

jjrico@legem.mx
irglobal.com/advisor/juan-jose-rico
+52 81 8143 0700

As a Chief of Compliance and Ethics at Legem Attorneys At Law, Juan José has expertise in diverse legal fields in Mexico related to business legal obligations as well as internal regulations. A lecturer on both legal and soft-skills matters, Juan José focuses his practice advising clients on compliance and technology regulation, tackling a wide variety of laws for mitigating legal risks.

Dr. Rico holds a Bachelor in Law as well as masters in Business and Public Management. In 2011 he was awarded his Ph.D. in Public Policy, in addition to more than 20 diplomas from different universities in the US, Canada, Mexico, and Europe.

legem.mx/en

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

In Mexico's case, the main challenges in terms of data privacy are:

- That government offices, companies and individuals understand the importance of protecting their personal data and their privacy. This information can be used improperly by third parties affecting their privacy as well as causing damage to their assets.
- The development of expert attorneys in data privacy regulation in different sectors such as government, companies as well as private practice.
- The development of cybersecurity experts.
- Fighting crimes related to the theft of personal information through information technologies.

One of the factors that impact the area of data privacy the most is the use of technology. Devices acquired and used by people every day are obtaining and sending their data to third parties without them agreeing or even being aware of it. The Internet of Things is a technological phenomenon that is a good example of the above.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

In the case of Mexico, the enforcement of data privacy is done through an autonomous government office (INAI) that receives complaints from people who feel concerned about their data privacy rights. Besides, there are autonomous local offices that also have certain faculties regarding data privacy. The national office coordinates with the local offices to carry out the work of law enforcement.

Once a complaint is filed, the INAI begins an investigation process and if irregularities are found in data privacy management, it proceeds to apply the corresponding sanctions. Based on the INAI resolution, the affected party or parties initiate lawsuits to request compensation for the improper use of their personal data.

In the case of Mexico, data privacy authorities have focused their efforts on letting people know the importance of protecting their privacy and their personal data. On the other hand, companies have been invited to also develop their own data privacy areas.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

The impact of the GDPR has been very important in Mexico since European companies that have operations in Mexico, especially those based on technology, have had to invest great efforts to harmonise the GDPR with the Mexican regulation (which is extensive and complex), especially because of the data traffic of employees, expats or customers.

This is mainly because many of the servers or data processing areas are in European countries or in jurisdictions where there is no regulation regarding data privacy or the existing regulations are weak.

Legem Attorneys at Law, SC is a law firm comprising professionals who specialise in a variety of legal disciplines. They have offices in the north, bajio and central Mexico, ensuring the highest ethical, professional and commercial standards are maintained. Their commitment is to help clients grow by providing them with opportune legal services oriented towards protecting their personal, economic and commercial interests.

The firm's areas of practice include litigation in civil, commercial, criminal, family, administrative and tax law. This includes corporate, banking, immigration and real estate law, as well as compliance expertise covering topics such as money laundering prevention, protection of personal data, anticorruption, evaluation and management of legal and regulatory risks programmes.

Data Privacy in Mexico

1. Before obtaining a person's data, you must have a privacy notice that establishes the most important aspects of data collection and storage.
2. There is personal data that requires express approval from individuals to obtain it. For instance, those that refer to finances, health, among others.
3. To have a personal data management policy within the organisation.
4. To appoint a person responsible for complying with the obligations of data protection laws within the organisation.
5. To have internal administrative, physical, and technological data protection mechanisms.
6. If the data obtained in Mexico is to travel to another jurisdiction, it is necessary to comply with various legal and foreign provisions.

EGYPT

Mohamed Agamy

Managing Partner, Links & Gains Law Firm

m.agamy@linksandgains.com
irglobal.com/advisor/mohamed-agamy
+20 100 0064 769

Mohamed Mostafa Agamy is the founder and Managing Partner of Links & Gains. Agamy is a bilingual lawyer and a driven professional legal consultant, with a proven track record of more than 15 years, leading successful international legal transactions. Agamy has a particular expertise in the North African and Middle East business markets.

Prior to establishing Links & Gains, he was responsible as Regional Counsel at General Electric and was the Head of Legal at BG (Shell) & Petronas LNG Downstream JV. He had successfully led negotiations and closure of settlement agreements to preserve and enhance shareholder value and resolve complex disputes. He demonstrates professionalism with an astute legal analysis and reasoning regions and countries and monitors disputes before Egypt Courts, CRCICCA, ICC, Dubai courts and England & Wales Courts.

linksandgains.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

The biggest challenge relates to applying law to new technology and businesses will need to understand areas of compliance with regards to obligations imposed on data controllers and processors. For instance:

- What data has been collected and for what purpose?
- What mechanisms and internal policies are in place that govern and control collecting and retaining personal data? When should it be updated? And when and how should it be destroyed?
- What are the most efficient ways of securing data for a particular retention period?

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

According to the proposal of the Data Protection Law that was approved by the Prime Minister in 2019 and subject to the Egyptian Parliament's final approval, the potential penalties include imprisonment, fines, and/or both. Fines vary from EGP 100,000 to EGP 5,000,000. Imprisonment terms vary from one to three years. So, for instance, "Any entity that violates Article 14, which bans the transfer of personal information to another country, could be fined between EGP 300,000 and EGP 3 million."

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

The main legal aspects of the GDPR have had a big impact in terms of influencing Egyptian legislators drafting the new data protection law for 2019. The proposed draft, for example, stipulates terms that offer a good framework for application, such as:

- The definition of personal data.
- The scope of application; if the data is partially or electronically collected by a controller and processor relating to all natural living persons in Egypt as well as non-Egyptians residing in Egypt.
- The creation of the data protection centre, "the Information Technology Industry Development Agency", which will regulate data protection, issuing licenses, ensuring the compliance of data protection laws and overseeing complaints.

LINKS & GAINS
ATTORYNEYS AT LAW

Links & Gains is an independent, full legal services law firm based in Egypt with connections to a number of international law firms and legal advisors. Our core area of expertise is commercial, and we have an outstanding track record in advising major local and international businesses on transactions in a range sectors. These include:

Aviation | Banking & Finance | Capital Markets | Corporate & Commercial | Energy Laws | Digital Technology | Dispute Resolution (Arbitration & Litigation) | Employment law | Insurance| Intellectual Property Rights | International Foreign Investment | Merge & Acquisition |Oil & Gas| Projects & Infrastructure | Real Estate | Renewables | Taxation | Transportation

Links & Gains has a standard of excellence that we bring to our clients and our network of legal firms. With a host of specialised services, our comprehensive understanding of business across different industries benefits our diverse client base.

| Data Privacy in Egypt

Although Egypt is currently looking to draft a new law on data protection, the new cybersecurity law – the Anti-Cyber and Information Technology Crimes – was issued under No. 175/2018 (Cybersecurity Law) that includes general provisions governing the confidentiality of personal data.

This is in reference to the Egyptian Constitution which stipulates mandatory principles that protect the individual's right to privacy including; correspondence, telephone calls, and other means of communication that may not be monitored, unless by a prior judicial permit. Financial institutions have been made to comply with the banking laws and regulations of the Central Bank. Other laws in Egypt have also penalised the breach of data protection such as the Labour Law, Telecommunication Regulation, Civil Code (In terms of damages for the private data infringement), plus certain penalties under the Penal Code (for the unlawful recording of calls or collecting of images).

US - NEW YORK

Della M. Hill

Associate, MacDonald Weiss PLLC

hill@macdw.com
irglobal.com/advisor/della-m-hill
+1 646 513 3280

An associate at MacDonald Weiss in New York City, Della M. Hill works on privacy, corporate, M&A, commercial, licensing, tax, and other business-related matters for US and international clients.

Della is certified by the International Association of Privacy Professionals (CIPP/US) and devotes a substantial amount of her time advising clients on the complex regulatory framework applicable to consumer-facing businesses. She provides guidance and support for compliance with US state and federal laws relating to data privacy, e-commerce contracts, marketing and promotional campaigns such as sweepstakes and contests, social media content, endorsements, and influencer campaigns, and other highly regulated consumer-based business activities.

macdw.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

New York is strongly focused on data privacy, but the law is still developing. The great challenge for affected businesses is dealing with the uncertainty about how the law will balance pro-consumer and pro-business interests—and what precisely it will require for compliance.

New York has passed a number of specific laws relating to data privacy and security, reflecting an increased commitment to the protection of consumer data. For example, the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act"), which strengthens and expands data protection and breach notification requirments, was signed into law this year.

However, a proposed comprehensive state privacy law (the "New York Privacy Act" or "NYPA"), referred to the New York State Senate Consumer Protection Committee for consideration, has faced strong resistance from business-oriented lobbyists. The NYPA has similarities with – and in some ways goes beyond – both the California Consumer Privacy Act ("CCPA") and the European General Data Protection Regulation. Although the proposed law failed to pass during the last legislative session, pro-consumer groups are strong and vocal in New York, and the NYPA may reappear in 2020.

Another challenge is that any New York-based company with an online presence is almost certainly reaching customers throughout the US and thus almost certainly is required to comply with multiple US privacy laws beyond those of New York. The patchwork nature of US privacy law, and especially the inconsistencies between the laws of the various states, makes compliance difficult. This challenge will become only more difficult to manage in the next decade, especially as technology continues to develop, unless Congress acts to pre-empt state law in this area or unless the states agree to follow common principles (as they have in some areas of commercial law).

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

New York has demonstrated an increased commitment to the enforcement of data privacy and security rules. In September 2019, the New York Attorney General filed suit against the parent company of Dunkin' Donuts for failing to safeguard the data of thousands of customers who were targeted in a series of cyberattacks, stating in a press release: "My office is committed to protecting consumer data and holding businesses accountable for implementing safe security practices."

The recently passed SHIELD Act increased civil penalties for violations of breach notification requirements and extended the statute of limitations on enforcement actions. Any business that collects personal data of New York residents will need to pay particular attention to compliance obligations under this new law, which applies to any business – regardless of size or location – that collects personal data of New York residents.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

One immediate impact of GDPR is that New York-based companies with a global customer base must decide whether to comply with the GDPR for all customer data collected (for example, obtaining explicit consent from both US and EU customers for the processing of certain types of data), or to maintain separate databases and offer differing degrees of protection to each. The latter may be difficult in practice, as it requires, for example, multiple versions of web pages on a global e-commerce website.

A more consequential impact of GDPR may be that New York consumers have become increasingly aware of the expansive (and potentially unchecked) collection, use, and disclosure of their personal data and, learning of the measures to protect the data of EU consumers under GDPR, may have developed expectations for similar protection in the US. The proposed NYPA is evidence of this impact.

Although it may be challenging for New York companies to build procedures that are simultaneously compliant with US law and the GDPR, it does provide an opportunity for international cooperation because this is the first time, generally speaking, that US companies without foreign branches or subsidiaries have had to pay attention to non-US law.

MacDonald Weiss offers a compelling combination of elite multinational law firm and Fortune 100 in-house experience, an accessible and nimble style, and value for money. In short, top tier sophistication on a human scale.

We serve mid-market companies, start-ups and emerging companies, family offices, angel, VC, and private equity investors, and large companies for whom a large firm is overkill for the task at hand. We focus on overseas clients with US activities, companies expanding into or out of the US, domestic early-stage companies, and investors.

MacDonald Weiss covers the core business-related practice areas: corporate, M&A, securities, finance, commercial, and tax. We also act as US – or global – outside general counsel.

| Data Privacy in New York

1. Pay attention to the overall data privacy framework

Pay close attention to the rapid developments in data privacy law – both in and outside of New York. A business collecting data from New York residents will likely need to comply with laws from multiple sources at the federal and state level (and, in some cases, with GDPR).

2. Know (and revisit) your client's data practices

Data flow mapping is a crucial step toward compliance. You must understand your client's practices for the collection, use, and disclosure of data (and any changes in these practices) to identify the data privacy laws that may apply at any given time.

3. Make sure your client follows through

Once your client's privacy practices are communicated to consumers, for example, in a website privacy policy, your client must actually follow the practices described. Failure to do so may not only lead to violations of the applicable privacy laws, but it may also violate the Federal Trade Commission Act, which requires that a company actually follow through on its promises and representations to consumers.

4. Do not forget service providers

Your client may be liable for data privacy violations by third parties engaged to collect, process, manage, or store customer data on your client's behalf. You should review any agreements between your client and such parties (e.g., cloud service providers) to ensure that they are contractually obligated to meet applicable data privacy obligations when acting on your client's behalf.

GERMANY

Dr. Dennis Voigt

Partner, MELCHERS Rechtsanwälte

d.voigt@melchers-law.com
irglobal.com/advisor/dr-dennis-voigt
+49 69 653 00 0663

Dr Dennis Voigt is an expert in data protection/GDPR-Compliance, IT/IP, distribution and advertising law. He has many years of experience advising on and offline businesses on how to set up and manage (trans) national distribution structures.

He particularly advises clients in the IT-/Software-industry, insurers, commercial/consumer goods manufacturers and retailers. Dr Voigt also offers expatriate services (inbound and outbound). He is a Recommended Lawyer 2019 in Legal500 Germany.

Dr. Voigt is based in Frankfurt am Main.

melchers-law.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

The biggest challenge of data privacy in Europe is to explain its own benefits as well as its actual regulatory content to the general public. The general public was annoyed after getting swamped by Data Protection Information Sheets in May 2018. Since then, the GDPR has been perceived (and blamed) by many as a regulatory monster prohibiting even the most innocent processing of personal data. The GDPR, however, does neither oblige data controllers to send data protection information sheets to existing customers, nor does it prohibit the processing of personal data.

The greatest challenge for data privacy, however, is its internationalisation. Unless there is a global level of data privacy, businesses may tend to move to jurisdictions without a reasonable level of data protection and thus avoid the additional costs of data privacy compliance; this may have an impact not only on the employment market but also the general environment for start-ups.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

The German regulatory authorities had organised themselves in order to comply with the requirements of the GDPR and at the same time had to answer the myriad of questions data controllers and data processors raised for clarification. It was therefore not particularly surprising to see that the German data protection authorities did not initiate a lot of proceedings due to a breach of the GDPR in 2018. However, German data protection authorities have just recently published a new guideline on how to determine penalties and fines in case of a breach of the GDPR. It is therefore safe to say that we will have to expect an increase of fines and penalties imposed on data controllers and data processors alike in the near future.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

The GDPR is the start of an ever increasing public awareness and public discussion of data protection matters, which began in 2007/2008 and led to a first modification of the national German Law on Data Protection in 2009 and then extended to the online collection and use of personal data. Data protection was already a hot topic when the GDPR entered into effect – however, the extremely high fines propelled data protection to the top of the list of topics discussed.

The data protection authorities in Germany have undergone a tremendous and substantial change. This does not only mean that data protection authorities have expanded their headcount and professionalism, but also their self-confidence in terms of imposing fines on data controllers of data processors alike. The GDPR has also forced the German data protection authorities to look beyond German borders. Some representatives of German data protection authorities have lately even been heard benchmarking the German authoritative approach with, for example, French data protection authorities.

MELCHERS

RECHTSANWÄLTE

MELCHERS is a full-service law firm with offices in Heidelberg, Frankfurt/Main and Berlin. About 50 commercially oriented, specialised attorneys advise clients in all areas of national and international business law. We regularly represent major (inter)national enterprises, medium-sized companies, public clients, start-ups and high net worth individuals.

Our practice focuses on all areas of corporate law, including mergers, acquisitions and private equity transactions, finance and capital markets, employment, distribution, property and construction, IP and IT law, data protection, general commercial law, insolvency, product liability and litigation. MELCHERS also supplies legal services in commercial criminal law and tax law – both in court an out-of-court.

MELCHERS ensures that partners actively contribute to client matters rather than merely supervising associates' work. We achieve this objective by keeping a high partner-to-associate ratio. We attach great importance in both individual and highly qualified legal advice, so each client has his own permanent contact partner who assembles specialised teams depending on the special needs of the current case.

| Data Privacy in Germany

1. Keep calm: GDPR-Compliance does not happen in one day and is a constant process.
2. In case of any doubt, seek contact with the data protection authority.
3. Establish a Data Protection Organisation in your business.
4. Draft a Data Protection Concept as a guideline and starting point for GDPR-compliance.
5. Unleash the tremendous hidden value of GDPR-Compliance:
    - document and get to know your business processes
    - improve, automate and simplify your business processes
    - professionalise and use data bases with personal data.

Divya Balagopal

Senior Partner, Mundkur Law Ptns.

dbalagopal@mundkur.com

+91 80 4357 6709

Divya Balagopal is the firm's co-founder and senior partner. She heads its education law, regulatory compliance and policy development practices.

Divya enjoys exploring new avenues and creating linkages – often taking the firm's expertise to areas not traditionally associated with corporate law firms. For instance Divya was the lead legal expert in the team that MLP fielded in South Sudan in 2013 to assist the then newly-formed nation on child rights and related issues. MLP's education law practices provides end-to-end legal services to educational institutions, investors, governments, and businesses in both e-learning and brick and mortar educational spaces.

Nandita Bhakta

Counsel, Mundkur Law Ptns.

nbhakta@mundkur.com

+91 80 4357 670

Nandita is counsel at Mundkur Law Partners, and works extensively on the firm's M&A, corporate and dispute resolution assignments.

She has assisted corporate entities in domestic and cross border M&A and private equity transactions, establishing compliance with Indian regulatory regime, and drafting and negotiation of commercial agreements for clients engaged in the financial services, information technology and education sectors. She has also represented clients before civil courts and arbitral tribunals in commercial disputes.

mundkur.com

QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

India does not have any data privacy specific legislation in force. Data privacy rights have to be culled from different legislations. The right to privacy was only recognised as a fundamental, constitutional right in 2017 when the Supreme Court of India delivered a landmark judgement. Prior to this, enforcement of the right to privacy was primarily through tort law and select legislations.

In 2017, the Supreme Court held information privacy to be a subset of the right to privacy. The court stressed the need for a comprehensive regulatory framework for data protection, balancing privacy concerns against legitimate State interests. This led to the 'The Personal Data Protection Bill, 2018' (PDP Bill). At the time of writing this article, the PDP Bill, is pending before the parliament of India for legislative assent. Once it becomes law, India will have its first integrated and focussed data protection regulation. Until then, some of the key challenges to data privacy in India include the following.

- Sector specific and varied standards: data privacy levels vary across different sectors such as banking, health, telecommunications and such varied standards lead to qualified protection to consumers and businesses.
- Varying standards of data protection for different data controllers and processors.
- Even statutes with similar standards may differ on enforceability. For instance, not every statute provides for remedies in cases of breach of data privacy.
- Statutory remedies are often seen as laborious, outdated and not cost effective in the long run, therefore enforceability is considered poor.
- Data privacy often has to be protected through contract negotiations.
- Protection of rights of internet users, e-consumers and cross-border data flows is, therefore, often complex and may require a large degree of customisation and contract negotiation.

In short, fragmented laws on data privacy and the absence of a comprehensive data privacy focussed legislation is at present India's biggest challenge.

QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

India's first infotech related law, the Information Technology Act, 2000 (IT Act), did not refer to data privacy. It was framed to give legal recognition to e-commerce within India. To a limited extent, this changed with two subsequent legislations: the Information Technology (Amendment) Act 2008 (2008 IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.

Data privacy is most prominently addressed by the laws on 'sensitive personal data'. Under Indian law, if the body corporate is negligent in implementing and maintaining reasonable security practices and procedures to protect 'sensitive personal data' and thereby causes wrongful loss or wrongful gain to any person, it will be liable to pay damages by way of compensation to the person affected. Similarly, data privacy is also covered to a limited extent by recognising intermediary liability and new offences such as using or retaining information from a stolen computer resource or communication device etc.

Under these laws, reasonable security practices and procedures have been defined to include security practices and procedures existing to protect information from unauthorised damage, use, modification, disclosure or impairment as specified in either the agreement between the parties or under any law in force or as prescribed by the central government.

These legislative protections are limited and inadequate in today's context and rapidly changing technology. This gap is currently being addressed during contract negotiations (especially on issues such as the standard of security, quantum of indemnity or damages). For example, while under the IT Act (by way of the 2008 Amendment Act), unauthorised access is prohibited, these regulations do not address protecting the integrity of customer transactions. If required this would need to be addressed by contract. The protection of the IT Act is also specifically not available in certain instances[1].

In summary, the current regulatory landscape on data privacy is piecemeal and inadequate.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

The proposed PDP Bill addresses the challenges and shortcomings of data protection regulations in India. Modelled after the European Union's GDPR, the PDP Bill focuses on all the key principles laid down under the GDPR such as privacy by design, transparency in processing of personal data, extraterritorial application, introduction of an adjudicating authority for data protection and prescribes high penalty for breach, i.e., a fine extending up to, a higher of 2-4% of the worldwide turnover for the preceding financial year or INR 5 to INR 15 crore (approx. $700,000 to $2 million) along with a compensation mechanism for data subjects.

That said, there are also a few key differences between the proposed law and GDPR, such as the right to be forgotten under PDP Bill does not include the data subject's right to data erasure, and contractual relationship is not a ground for processing personal data. Other significant provisions of the proposed legislation include the restrictions on cross-border data transfer and processing, although such transfers will be permitted subject to consent from data subject and approval from a designated authority on statutory grounds which include adequacy, standard contractual clauses/ schemes and necessity. Additionally, the proposed law imposes data localisation obligations, i.e., requirement of storage of a copy of all data on the local server of the data processor or controller. Further, for safeguarding certain categories of sensitive data additional obligations restricting foreign processing may be placed by the government at a later date.

The road ahead for data privacy in India looks promising, although the effectiveness of the legislation can only be tested on its implementation. In its current form, the proposed law slightly diverges from GDPR with its additional obligations dealing with restrictions on data transfer and processing. For operational reasons, however, the PDP Bill complements GDPR and therefore the cost of transition to comply with the proposed Indian data protection law will be minimal for multinationals that are already GDPR-compliant, and any further complexities in operation of the law and its impact on entities complying to laws of multiple jurisdictions will only surface in due time.

1 *Execution of Negotiable Instrument under Negotiable Instruments Act, 1881, except cheques; Execution of a Power of Attorney under the Powers of Attorney Act, 1882; Creation of Trust under the Indian Trust Act, 1882; Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition; Entering into a contract for the sale of conveyance of immovable property or any interest in such property; Any such class of documents or transactions as may be notified by the Central Government in the Gazette.*

MLP
MUNDKUR LAW PARTNERS

Mundkur Law Partners (MLP) is an award winning corporate law firm based in Bangalore, India. The firm specializes in complex, international transactions, and is reputed for adding exceptional value in developing client strategies (in both transactions and disputes). The firm's clients range in size from listed multinationals to start-ups, with interests across diverse areas—from brick and mortar manufacturing to cutting edge drug-discovery and technology-based businesses.

The firm's practice focusses on five areas: international M&A (including private equity and venture capital transactions), education law, life sciences and healthcare, insolvency resolution and complex commercial disputes. The firm values its strong reputation for exceptional client service, and offers each client the assurance of complete partner involvement in every aspect of the client engagement.

| Data Privacy in India

1. When in doubt use GDPR or the provisions of the PDP Bill to benchmark compliance (even if this exceeds the scope of currently applicable law in India). The current framework on data privacy will change. The cost of implementing a data protection system is still relatively low in India. Benefits range from efficiency in cross-border commerce, increased confidence in business.
2. Focus on prevention policies and good practices to promote data privacy with the same rigour as response protocols for breach. Data privacy is often seen only as a technology issue, but protection practices/governance and compliance education are critical for prevention; as are clear, easy, visible protocols to address any breach of data privacy.
3. Negotiations for data privacy needs to be included as standard practice in contract negotiation.
4. Sector specific obligations applicable for data protection must be examined and followed for compliance.
5. Trade-offs between the right to privacy/ commercial value of data/ governmental rights is an ongoing issue, and it is important to note that the rules regulating content on intermediaries and on social media are to be finalised by the government early next year.

AUSTRALIA

Matthew Shearing

Associate, Rouse Lawyers

mshearing@rouselawyers.com.au
rouselawyers.com.au/our-team/matthew-shearing
+61 7 3648 9900

Matthew Shearing is a technology and commercial lawyer with Rouse Lawyers.

Much of his work involves companies that use technology as a key part of their business – from managed services and consultants to cybersecurity and esports. He runs an emergent technology podcast, consults on blockchain technology and is an advocate for free and open-source (FOSS) software.

He's a member of Blockchain Australia, the Australian Information Security Association and Queensland Law Society.

rouselawyers.com.au

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

Make no bones about it – the past decade has been the decade of data abuse. From monetisation through Facebook and Google to secret government initiatives like the NSA's PRISM, data privacy hasn't been very well respected these last 10 years.

It's hard to see this trend reversing course for the next decade. Reliance on services which monetise personal data is increasing, from Facebook Messenger to Amazon Alexa. Intelligence legislation is also becoming increasingly draconian (more on that below). But perhaps the biggest challenge for data privacy will come from the many new ways data will be used in the next decade.

The buzz in Australia around 'Smart Cities' is a perfect example. The premise sounds great – an interconnected metropolis where cars park themselves, streetlights sense movement and traffic flows freely. Powered by communications technology like 5G and mesh networking, it promises a world where everything is connected and working in complete harmony.

But to facilitate such an endeavour, it will mean collecting an unprecedented amount of data – most of it personal. Systems will need to know where citizens are at all times, tracking their every move. AI algorithms will recognise faces and traits, matching them to a personal profile. They'll pay attention to what people do, what they focus on and who they interact with.

This will obviously provide huge opportunities for both the public and private sector. Governments will be able to automatically monitor citizens and fine them whenever they break a law. Companies will have a behavioural profile that would make current advertisers salivate.

It will be challenging to maintain privacy in an increasingly connected and data-rich world, but we believe there's a huge opportunity for privacy-respecting businesses to differentiate themselves.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

Strengthening Privacy Law

The Notifiable Data Breach scheme (NDS) continues to be the an effective framework for data breaches in Australia. Recent changes in the NDS allow regulators to fine companies up to $10 million AUD for concealed data breaches – which may have been what prompted Australian unicorn Canva to immediately notify approximately 140 million users when they discovered a massive data breach in May this year.

Unfortunately, there's still a general apathy around protection of user data – and actual regulatory action is relatively low. This is despite Australia having overwhelmingly the highest rate of data breaches in the Asia-Pacific region.

One difficulty facing regulators is that unless a data breach is shared or publicised by the breaching party, many companies either don't know (or don't want to share) their breaches. Most reported breaches are examples of companies doing the right thing and following the scheme – so enforcement action against them would be counter-intuitive.

Attack on Encryption

While we've made some notable improvements in data privacy regulation, there's been some equally confusing steps backwards. While implementing the NDS, the Australian Government was concurrently crafting the Assistance and Access Bill, which was rushed through Parliament at the end of 2018 despite general outcry from the tech sector.

The legislation allows intelligence agencies and police to serve notices on companies which require building secret backdoors, automated information sharing mechanisms, vulnerabilities or even sharing encryption keys. Anyone that refuses faces up to 10 years jail time and very hefty fines.

Not only is the potential for abuse of this system plain (there is little to no judicial oversight), it requires companies to essentially hack their users, share data in secret and leave their systems wide open to exploitation. Encryption is an essential function of modern business because it protects data privacy – and the new legislation means that companies will be easy targets for hostile actors.

This is a trend we are continuing to monitor, and one which makes for a very schizophrenic legislative framework.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

It's hard to say the GDPR has been anything but a resounding success. Even here in Australia, far removed from the European Union, many businesses have altered marketing practices and become savvier with data handling.

It's also forced regulators to change. The Australian Government has taken a number of steps to move closer to the EU, including several pieces of draft legislation which will:

- require that customer data be transferred securely;
- require accreditation for receiving and processing certain types of data;
- require destruction of unsolicited data;
- prohibit use certain data for direct marketing; and
- heighten requirements for companies to protect data from misuse, interference, loss, unauthorised access, modification or disclosure.

The first leg of this legislation will be rolled out under the guise of an 'Open Banking' system, requiring the larger banks in Australia to incrementally share their product data publicly. If all goes to plan, it'll mean more consumer visibility and, thus, more competition.

We've also seen the Australian Cyber Security Centre (an intergovernmental cyber security agency) take increasing responsibility. In concert with similar centres internationally, they've released a steady flow of practical, workable information for businesses looking to shore up their data management.

Overall, international privacy regulation seems to be converging. While this may mean short term pain for enterprises as they come up to standard, the regulatory similarities should mean a more workable environment for everyone in the long run.

Rouse Lawyers is an Australian commercial law firm that stands apart as a real alternative to large law firms with bloated overheads and slow delivery.

We are a team of specialist lawyers working in an efficient, technology-driven practice environment that gives us the ability to deliver top tier results and true value to our clients. Rouse Lawyers maintains an edge in the market with a core group of commercial lawyers and a flexible network of external legal specialists based throughout Australia and New Zealand.

Data Privacy in Australia

1. **Change how you look at data.** Everything has a price – and people are paying big money for data. Treat data like holding physical gold.
2. **Review your policies often.** Regulation is rapidly changing, as are the risk profiles. You should be reviewing at least twice a year.
3. **Take some serious steps to secure the data that you store.** Focus on your biggest weakness – you and your employees. Get training early and often. Encrypt everything.
4. **Have a plan in place.** Data breaches are incredibly stressful, and your actions dictate the response of customers & regulators later. Planning ahead can make all the difference.
5. **Ask if you really need the data you're collecting at all.** Too many companies collect data without giving thought to the risk they're taking on. Do you actually need a customer's full name and address? Could you use a third-party payment processor? Less data = less risk.

BELGIUM

Joost Peeters

Partner, STUDIO | LEGALE

joost.peeters@studio-legale.be
irglobal.com/advisor/joost-peeters
+32 3 216 70 70

Joost PEETERS, co-founder and associate of STUDIO | LEGALE, started his Law Studies at the University of Antwerp (UA, Belgium) and graduated via the University of Leuven (KU, Belgium) at the University of Rome (LUISS Guido Carli, Italy) prior to joining the Antwerp Bar in 2001.

He specialised in Insurance Law, Company Law (assistance in various takeovers and share transfers), Business Law, (Commercial) Tenancy Law, Contract Law, and Traffic Law. He attended the post-graduate course for Receivership Practice and assists companies in difficulties (mainly in cases governed by the Belgian Continuity of Enterprises Act). He was sworn in as Deputy Justice of the Peace in Antwerp and is also a Legal Assessor for the Belgian Architects' Association, a Receiver and an Administrator.

Joost Peeters is holder of the Special Training Certificate for Belgian Criminal Cassation Proceedings, speaks Dutch, French and English fluently and can get by in Italian.

Joost is also a holder of the Data Protection Officer (DPO) certificate, awarded by the renowned Data Protection Institute (DPI).

studio-legale.be

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

One of the biggest challenges is creating awareness about data privacy. Because of the cautious start of the Belgian Data Protection Authority, a lot of companies failed to conform to the GDPR. Many organisations believe that receiving a fine for non-compliance is rather remote, at the moment at least. A lot of these companies will keep refusing to comply with the GDPR as long as there is no incentive. That is why it is important to create more awareness about data privacy. Companies have to understand why they need to be careful with the data they collect. This awareness will be created when the Belgian Data Protection Authority takes more actions against violators. It is better to be safe than to be sorry, which is why it is important the awareness is created before the Belgian Data Protection Authority takes a harder line against violators.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

When the GDPR was implemented, the Belgian Privacy Commission was transformed into the Belgian Data Protection Authority. With this transformation, more power was given to the Belgian Data Protection Authority in order to have an authority with the proper opportunities to enforce data privacy breaches.

The Belgian Data Protection Authority started off rather cautiously. The first cases were all concluded with a warning for the violators. Recently, the authority imposed two fines (one of €2000 and one of €10.000). It is expected that the authority will exercise its powers to sanction violators more.

I QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

At this moment the impact of the GDPR in Belgium has been small. In addition, those companies fined for non compliance have yet to be sanctioned, giving people the impression the GDPR is not too important. But it is expected the authority will exercise more powers, which give GDPR more relevance.

Since the GDPR is still in its early stages, it is difficult to make a judgement about the efforts at international cooperation. Some of the national authorities have already been very active at enforcing the GDPR, while others still need to start enforcing it. But of the 13 decisions the Belgian Data Protection Authority has taken, three of the complaints were cross-border complaints that were transferred by other national Data Protection Authorities.

STUDIO | LEGALE Advocaten www.studio-legale.be

STUDIO|LEGALE (°2009) is a dynamic law firm with one single objective: to assist you quickly and pragmatically in your legal matters. We have 18 lawyers and five administrative staff available to help you. In Belgium, you can find us in Antwerp and in Brussels, at both locations near the palace of justice.

STUDIO|LEGALE is a legal ONE STOP SHOP, with various specialists under the same roof

Areas of expertise are: Insurance Law; Debt & Asset Recovery; Data Privacy & Security; Retail and Real Estate; M&A.

| Data Privacy in Belgium

1. Create awareness: in order to smooth the data privacy process, people need to be aware of the importance of data and why it needs to be secured. At this moment, the importance of data privacy is neglected by many people, which leads to a lot of organisations failing to comply with the GDPR.
2. Use the GDPR to smooth your company's processes, see it as an opportunity: do not see the GDPR as a burden to your company. When you try conforming your company to the GDPR, it is an excellent reason to screen your company's processes. It will help you to get rid of data you don't need and which only slows down your activities. By complying with the GDPR, you will know where your data are, which data you have, and what you can do with that data.
3. Train the people working with data: human actions are a huge liability for data privacy. That means it is important that people who work with data are well trained. They need to know the importance of data privacy, how to handle data and what to do when something goes wrong.
4. Be proactive: when an organisation is GDPR-compliant at one moment, it does not mean the organisation will stay compliant. As an organisation, you have to be proactive.
5. Take serious action: organisations need to take serious action in order to be GDPR compliant. Compliance is not just filling in some forms and storing them; it is much more than that. When organisations see the importance of data privacy, and take serious actions, data can be a real asset to the organisation.

Contributors (A-Z)

Mark Benton
Partner, AHNSE Law Offices
irglobal.com/advisor/mark-benton

Jesszika Udvari
Partner, Buzády & Udvari Attorneys at law
irglobal.com/advisor/dr-jesszika-udvari

Monika Naef
Partner, DUFOUR Advokatur
irglobal.com/advisor/monika-naef

Robert Lewandowski
Partner, DLP Dr Lewandowski & Partners
irglobal.com/advisor/robert-lewandowski

Yusuf Mansur Özer
Associate, ErsoyBilgehan
irglobal.com/advisor/yusuf-mansur-oezer

Aaron Allan
Partner, Glaser Weil Fink Howard Avchen & Shapiro LLP
irglobal.com/advisor/aaron-p-allan

Alexander J. Suarez
Associate, Glaser Weil Fink Howard Avchen & Shapiro LLP
glaserweil.com/attorneys/alexander-suarez

Sönke Lund
Partner, Grupo Gispert
grupogispert.com/en/team/soenke-lund

Anna Fernqvist Svensson
Partner, hellström advokatbyrå kb
irglobal.com/advisor/anna-fernqvist-svensson

Matthew Lea
Senior Solicitor, Herrington Carmichael
herrington-carmichael.com/our-people/matthew-lea

Henrik Christian Strand
Associate Partner, Holst, Advokater
irglobal.com/advisor/henrik-christian-strand

Adelina Dospinescu
Managing Associate, Hristescu & Partners
hmpartners.ro/crew

Lavinia Junqueira
Partner, Junqueira Advogados
irglobal.com/advisor/lavinia-junqueira

Cauê Rodrigues Amaral
Associate, Junqueira Advogados
jlegalteam.com

Oscar Conde
Managing Partner, Legem Attorneys at Law, SC
irglobal.com/advisor/oscar-conde-medina

Dr. Juan José Rico Urbiola
Counseling/Compliance, Legem Attorneys at Law, SC
irglobal.com/advisor/juan-jose-rico

Mohamed Agamy
Managing Partner, Links & Gains Law Firm
irglobal.com/advisor/mohamed-agamy

Della M. Hill
Associate, MacDonald Weiss PLLC
irglobal.com/advisor/della-m-hill

Dennis Voigt
Partner, MELCHERS Rechtsanwälte
irglobal.com/advisor/dr-dennis-voigt

Divya Balagopal
Senior Partner, Mundkur Law Partners
mundkur.com

Nandita Bhakta
Counsel, Mundkur Law Partners
mundkur.com

Matthew Shearing
Associate, Rouse Lawyers
rouselawyers.com.au/our-team/matthew-shearing

Joost Peeters
Partner, STUDIO | LEGALE
irglobal.com/advisor/joost-peeters

Contacts

UK HEAD OFFICE

IR Global
The Piggery
Woodhouse Farm
Catherine de Barnes Lane
Catherine de Barnes B92 0DJ

Telephone: +44 (0)1675 443396

www.irglobal.com
info@irglobal.com

KEY CONTACTS

Rachel Finch
Channel Sales Manager
rachel@irglobal.com

Andrew Chilvers
Editor
andrew@irglobal.com

IR GLOBAL
The Piggery, Woodhouse Farm, Catherine de Barnes Lane, Solihull B92 0DJ

+44 (0)1675 443396
www.irglobal.com
info@irglobal.com