

Key contacts

Spain



Blanca Escribano
Partner
+34 91 187 1924
blanca.escribano@olswang.com



Sofia Fontanals
Senior Associate
+34 91 187 1932
sofia.fontanals@olswang.com

Asia



Elle Todd
Partner
+65 9649 0449
elle.todd@olswang.com



Matt Pollins
Associate
+65 6422 2818
matt.pollins@olswang.com

Key contacts

United Kingdom



Ross McKean
Head of Data Protection
+44 20 7067 3378
ross.mckean@olswang.com



Claire Walker
Head of Commercial Know How
+44 20 7067 3174
claire.walker@olswang.com

Belgium



Christine De Keersmaecker
Partner
+32 2 235 0307
c.dekeersmaecker@olswang.com



Matthias Vierstraete
Advocaat
+32 2 235 0301
matthias.vierstraete@olswang.com

Germany



Andreas Splittgerber
Partner
+49 89 206028-404
andreas.splittgerber@olswang.com



Viola Bensinger
Partner
+49 30 700 171-150
viola.bensinger@olswang.com

For regular privacy news and comment from around the world follow our blog at www.datonomy.eu

- Berlin +49 30 700 171 100
- Brussels +32 2 647 4772
- London +44 20 7067 3000
- Madrid +34 91 187 1920
- Munich +49 89 203 031 300
- Paris +33 1 70 91 87 20
- Singapore +65 67 20 82 78
- Thames Valley +44 20 7067 3000

www.olswang.com

Data compliance

The Olswang Privacy Risk Assessment

OLSWANG



Why audit? The business case

Data privacy is a now a Board level issue. First, there is the “stick”: dealing with a major security breach and repairing the damage to a company’s hard-earned reputation is expensive. Fines may follow: currently up to £500,000 in the UK, with anti trust style fines of up to 2% or even 5% of global turnover proposed by the EU.

Counting the cost of a security breach

£450-850k	average cost to large organisation of worst security breach
£35-65k	average cost to small business of worst security breach
5% of global turnover fines proposed by European Parliament under draft GDPR	

Source: BIS/pwc 2013 Information Security Breaches Survey

The EU reforms will also drive organisations to have far greater visibility and documentation of the personal data they hold and the way they process it (see “Future-proofing for the new rules”). Targeted investment in prevention is more cost-effective than cure after the event.

Second, the carrot: with customer data now the key asset for most consumer-facing businesses, privacy compliance is also fundamental to data value and the ability to exploit information commercially.

The Olswang Privacy Risk Assessment

Key features

- Fixed pricing, according to scale and depth of review required
- User-friendly, dedicated, secure SharePoint site
- Legal advice privilege protection is maximised by channelling the review through Olswang
- Content based on EU rules and best practice, customisable to other territories
- Business-friendly questionnaires, structured by function
- Full audit trail of responses
- Information is gathered and submitted by your team, helping you manage costs

“Investment in prevention is more cost-effective than cure.”

What’s included?

- An initial review with your legal or compliance team to scope the project
- User-friendly launch presentation, guides and jargon-busters
- Online questionnaires for all operational functions and processes
- Evaluation of the review responses
- Gap analysis, prioritisation and practical remedy plans
- Legal and project management support throughout the process

A review tailored to your business

While the main operational functions are common to all businesses, each organisation will structure its operations differently. Understanding what personal data your organisation holds, and where responsibility for it lies, is key to an effective review. The questionnaires for the key operational functions can be tailored to reflect the way your business really works.

You may wish to review every area of your business – or you may decide to focus on certain high risk areas of data handling. The review can cover the following operations.

- Multichannel sales and marketing
- IT and information security
- Human resources
- Supply chain and procurement
- Finance and accounting
- Legal and other support functions
- CCTV
- Processes and functions specific to your business

Working with your team

Getting buy-in from your key stakeholders - typically the CIO, and heads of multichannel, HR, and their teams – is key. We’ll provide full training on how to use the site and de-mystify the legal jargon. The questionnaires have been developed with input from professionals in IT, HR, marketing and procurement and contain embedded guidance, prompts and examples relevant to each business function. But if your team have any questions, we are just a phone call or an email away.

“Privacy compliance is fundamental to data value.”

A multi -disciplinary approach

Data issues often call for expertise beyond black letter law. We can partner with experts in other disciplines to offer joined-up solutions to the challenges – and opportunities – inherent in data handling.

- Digital strategy and data analytics: enhancing online presence though more intelligent use of data
- Data security and cyber security: vulnerability testing and practical security measures to reduce the risk of a breach
- PR and communications: crisis and reputation management in the event of a breach

Working internationally

Our questionnaires are based on EU principles and best practice but can be tailored for other territories. Using our network of international offices and best friend firms – both in Europe and Asia - we can provide pragmatic advice informed by knowledge of local law and insight into local enforcement practice.

Future-proofing for the new EU rules

The proposed new EU Regulation looks likely to replace the current regime by as early as 2016. The final detail is still not set in stone, but stricter rules and competition style turnover based fines look certain. Proposed new obligations – which will drive the need for greater visibility and documentation of data handling – include:

- The Accountability Principle
- Appointment of a Data Protection Officer
- Privacy impact assessments for higher risk processing
- Privacy by design and default
- Paper trails of all processing
- Full documentation of data responsibilities in commercial agreements
- Up-front security risk evaluations
- More emphasis on privacy policies and consumer information

“The new EU Regulation will make greater visibility of data handling a must-have.”

A lifecycle approach to data management

Data is a business-critical asset. Problems typically come to light when data is disposed of carelessly, or used by organisations for purposes that an individual did not consent to. But problems can arise at any stage. Our risk assessment aims to highlight compliance issues wherever they occur in the data lifecycle – whether at the point of capture, disclosure to third parties, storage and ultimately disposal – and help you reduce risk.

