



PCTY2011



Pulse Comes to You

Optimising the World's Infrastructure

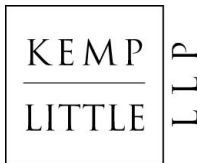


Information Management and Security

A Legal Perspective

Paul Hinton and Ivor Drake

10 May 2011



Introduction - Kemp Little LLP

Legal focus:

- Data Rights/Privacy/Security
- Intellectual Property
- IT and outsourcing
- Corporate (M&A/ Investment /Strategic Alliances/ Exits /Corporate Governance)
- Employment
- Litigation

Market focus:

- "UK IT law firm of the year 2010"
(Global Legal Experts, Oct 2010)
- Top UK specialist firm – FT Law 50
(FT Innovative Lawyers, Oct 2010)

A sample of the range of our clients includes:



Spot the Difference?

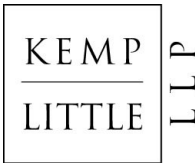
Lost Laptop A

Lost Laptop B



The Difference

- Lost Laptop A
 - Front page news articles
 - ICO Published Undertaking and Fine
 - Undertaking to improve ICO policies and agree to ICO Audit
 - System changed – laptops encrypted – remote deletion software installed
 - Laptop policy introduced
 - Customers informed and credit checks paid for
 - All Customer security details changed
 - Lost 15% of customers
 - IT Security Manager fired
- Lost Laptop B?



Overview

Part 1 – Introduction – why is data loss important

- Background
- Examples

Part 2 – Legal Issues

- Protections
- Obligations

Part 3 – Conclusions

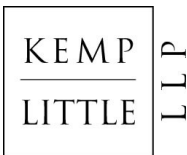
- Policies
- Practical tips
- Information Management Strategy

Information Management

- Information is a key asset of every business
- Technology has developed so fast that it can do most of what we want it
- Revolutionised our ability to access, create, store, search and communicate information
- The battle now is to control and exploit information to best effect
- **Information Management is in its infancy and lagging behind technological development**

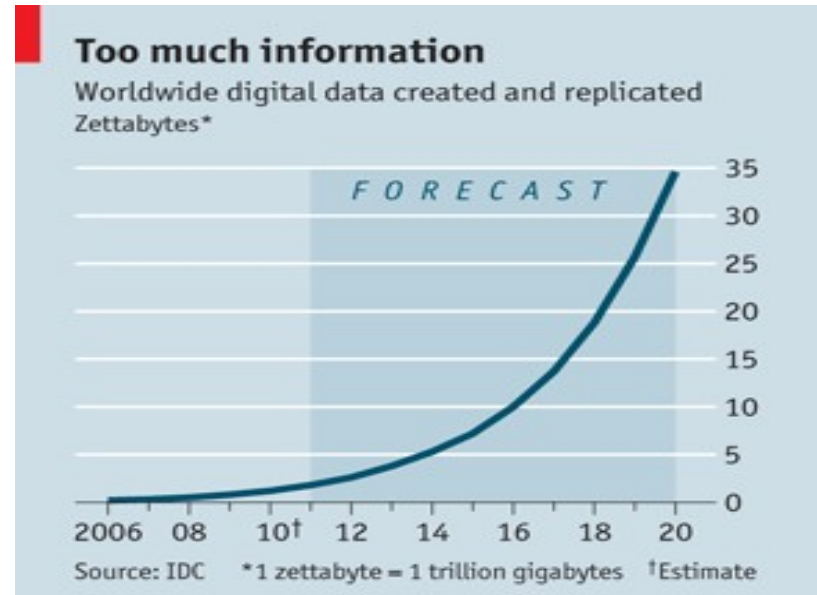


“the stone age was marked by man's clever use of crude tools; the information age, to date, has been marked by man's crude use of clever tools”



Amount of digital data...

- 2011 amount of global digital data estimated = 1.2 ZB
- 2020 amount of global digital data = 35 ZB
- **Zettabyte** = 1,000,000,000,000,000,000 bytes = $1000^7 = 10^{21}$
- Storage requirements for all human speech ever spoken = 42 ZB if digitized as 16 kHz 16-bit audio
- 85% held by businesses
- Average company keeps 60% more data each year



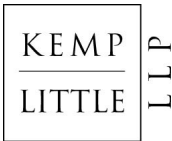
Storing up trouble

- Many organisations keep everything
 - Often bad habits rather than a corporate strategy
 - Lack of control over data
 - “Do not want to lose anything”
 - “Difficult to filter information”
 - “Easier to keep everything”



“PATHOLOGICAL HOARDING DISORDER”

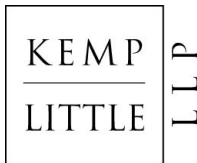
The acquisition of and failure to discard possessions that are useless or of limited value due to a fear of losing things perceived to be important.





Security Risks attached to Data

- 88% of companies experienced data loss in last 12 months
- 53% business laptop users carry confidential company information and 65% of those don't take protect the data
- Average cost of significant data breach estimated to be £4.5m per breach
- Estimated 67% of ex-employees take data to leverage a new job
- 514 million people affected by data loss since 2007



Data Loss/Theft (i) Employee accident

guardian.co.uk

Printing sponsored by:

Kodak
All-in-One Printers

GCHQ staff lost 35 laptop computers, report says

Intelligence security committee says 'haphazard' monitoring meant it was not known whether top secret information had been mislaid

Richard Norton-Taylor
guardian.co.uk, Thursday 11 March 2010 17:42 GMT

A latter / smaller



GCHQ's monitoring system has been criticised as 'haphazard' in an intelligence security committee report. Photograph: PR

Staff at GCHQ, the government's electronic eavesdropping centre, mislaid 35 laptops and it was not known whether the computers contained top secret information because of the agency's "haphazard" monitoring system, it emerged today.

KEMP
LITTLE

LLP

Data Loss/Theft (ii) “Malicious” Employee

Find a Job | Dating | Wine | Our Papers | Feedback | My Stories

Tuesday, Apr 05 2011 3PM 14°C 6PM 13°C 5-Day Forecast

MailOnline

Science & Tech

Home News U.S. Sport TV&Showbiz Femal Health **Science&Tech** Money Debate Coffee Break Travel Royal Wedding

Science&Tech Home | Pictures | Gadgets Gifts and Toys Store

Login

Wikileaks set to release new Iraq war logs 'seven times bigger than the first'

By DANIEL BATES
Last updated at 4:58 PM on 22nd November 2010

[Comments \(39\)](#) [Add to My Stories](#)

Wikileaks has announced it will release a third set of war logs which will be seven times bigger than the last batch.

In a defiant posting on its official Twitter account, the website's founders said it was 'under intense pressure' over the disclosure but vowed to press ahead anyway.

'The coming months will see a new world, where global history is redefined. Keep us strong,' they added.



Search Advanced Search



Headlines

Most Read

- Russian rocket Soyuz blasts off for International Space Station with U.S. astronaut aboard
- Egyptian mummies who lived 3,500 years ago 'had clogged arteries despite healthier lifestyle'
- Look for the mines! Scientists claim the best way to find alien life is to search for signs of engineering on asteroid belts
- The day the mobile phone went public 38 years ago, leaving New Yorkers bemused and bewildered
- That's enough for me: Scientists discover gene that influences drinking habits
- We're in for Wikileaks! Study finds games console...

guardian.co.uk

WikiLeaks has altered the leaking game for good. Secrets must be fewer, but better kept

For whistleblowers, government and press, the age of digileaks cries out for new rules on what to hide – and reveal



Timothy Garton Ash
guardian.co.uk, Wednesday 30 March 2011 21.00 BST

[A larger](#) | [smaller](#)

Suppose you know a secret that you think should be made public. How do you go about it? Suppose your organisation has secrets you believe must be guarded. What should you do? Suppose you are an editor, blogger or activist, with the whistleblower huffing in your left ear and a government or company puffing in your right. Where do you draw the line?

One answer to the first question comes from [Daniel Domscheit-Berg](#), a former member of the WikiLeaks team. His [OpenLeaks](#) initiative aims to provide an untraceable "digital dropbox" in which would-be whistleblowers can deposit their digital troves. However, OpenLeaks would not itself select and publish material, as WikiLeaks did when it edited – and titled [Collateral Murder](#) – a video taken from an American helicopter gunship in Iraq as it killed 12 people, including two Reuters journalists, and wounded two children.

KEMP
LITTLE

LLP

Data Loss/Theft (iii) Outsourced Supplier

The Telegraph

Search - enhanced by Google

HOME NEWS SPORT **FINANCE** COMMENT CULTURE TRAVEL LIFESTYLE FASHION TECHNOLOGY Jobs Dating Offers
Companies Comment Personal Finance Economics Markets Your Business Olympics Business Fund Game Business Club Blogs
Banks and Finance Media and Telecoms Retail Transport Construction Industry Energy Pharmaceuticals

Insurance

Zurich UK fined record £2.28m for losing customer details

The British arm of Zurich Insurance has been fined a record £2.28m for losing the financial details of 46,000 customers.



Photo: AP

By Louise Armitstead 6:30AM BST 25 Aug 2010

The Financial Services Authority (FSA) found that an **unencrypted back-up tape** containing customer details was lost in 2008 while being transferred to a data storage centre in South Africa.

It took a year for Zurich UK, which had outsourced the data processing to Zurich South Africa, to notice the error.

The regulator said that the "cumulative impact" of Zurich UK's failings "represented a material risk to the FSA's objectives of reducing financial crime and protecting customers".

Share:

Recommend

Tweet 1

Insurance

News » UK News » Finance » Banks and Finance » Business Latest News »

IN FINANCE



Insurance chief says industry needs a makeover



World's most expensive natural

Telegraph
wealth
management service

Contact 0800 953 5050 or click here for more information

Reserve your complimentary place today

MARKET DATA

UK	WORLD	FOREX	Chart period: 1d
FTSE 100	6,017 +0.1%		6035
FTSE 250	11,767 +0.5%		6022
All Share	3,122 +0.2%		6010
SmallCap	3,260 +0.3%		5997
AIM	907.4 +0.2%		

8 AM 10 AM 12 PM 2 PM 4 PM GMT © 2011 MoneyAM

Company share prices

RISERS AND FALLERS

RISERS	FALLERS
Banks & Finance	

KEMP
LITTLE
LLP

Data Loss/Theft (iv) Malicious “acts”

guardian.co.uk

Printing sponsored by:

Kodak
All-in-One Printers

Sony bosses apologise over theft of data from PlayStation Network

Sony plans a goodwill package offering users complimentary downloads and 30 days of free service around the world

Agencies

guardian.co.uk, Sunday 1 May 2011 16.32 BST

A [larger](#) | [smaller](#)



Sony Computer Entertainment president, Kazuo Hirai (C), and executives Shiro Kambe (L) and Shinji Hasejima, bow to apologise for the theft of personal data from users of the company's PlayStation Network and Qriocity online services, at a press conference at the Sony headquarters in Tokyo on 1 May, 2011. Photo credit Toru Yamanaka/AFP/Getty Images Photograph: TORU YAMANAKA/AFP

KEMP
LITTLE
LLP

Data Loss/Theft (v) Competitor Theft

NETWORKWORLD

This story appeared on Network World at <http://www.networkworld.com/news/2009/031909-high-tech-spy-case-trial.html>

Chinese high-tech spy case inches closer to trial

Software engineer Hanjuan Jin is accused of stealing thousands of confidential documents from Motorola

By [Ellen Messmer](#), Network World
March 19, 2009 05:48 PM ET

Did software engineer Hanjuan Jin, who worked at Motorola for about eight years, [steal](#) thousands of confidential and proprietary technical documents to share with competitor Lemko and the People's Republic of China?

Jin, in her late 30s, says she didn't. But U.S. federal prosecutors are going after her for allegedly sharing technical and highly-sensitive trade secrets to benefit a "foreign government, namely the People's Republic of China, specifically its military," according to the Dec. 9, 2008, indictment filed by federal prosecutors in Chicago.

While the U.S. government's legal paperwork seeks to shield identity by referring to the victim firm as simply "Company A," it's a safe bet that it's Motorola, which has its own civil lawsuit pending against Jin and cellular-equipment maker Lemko with many identical details -- though it doesn't accuse her of sharing secrets with the Chinese government.

The shroud of secrecy will officially drop once a public trial begins; federal prosecutors and Jin's attorneys are due to meet in a Chicago court next week with the expectation of setting a trial date.

The insider threat

Jin was arrested by U.S. Customs officials on Feb. 28, 2007, at Chicago O'Hare International Airport, ready to depart on a one-way ticket to China. She was carrying over 1,000 electronic and paper documents from her former employer -- she had just quit Motorola -- as well as Chinese documents for military telecommunications technology, according to the Federal Bureau of Investigation (FBI) affidavit filed in court as part of the case.

That's the heart of the feds' criminal lawsuit against Jin, a U.S. citizen born in China, who was released on \$50,000 bail.

Sponsored by:



IBM System x3650 M3 Express Server

With the Intel® Xeon® processor 5600 series
From \$2,929 or \$75/mo

Learn more ►



KEMP
LITTLE

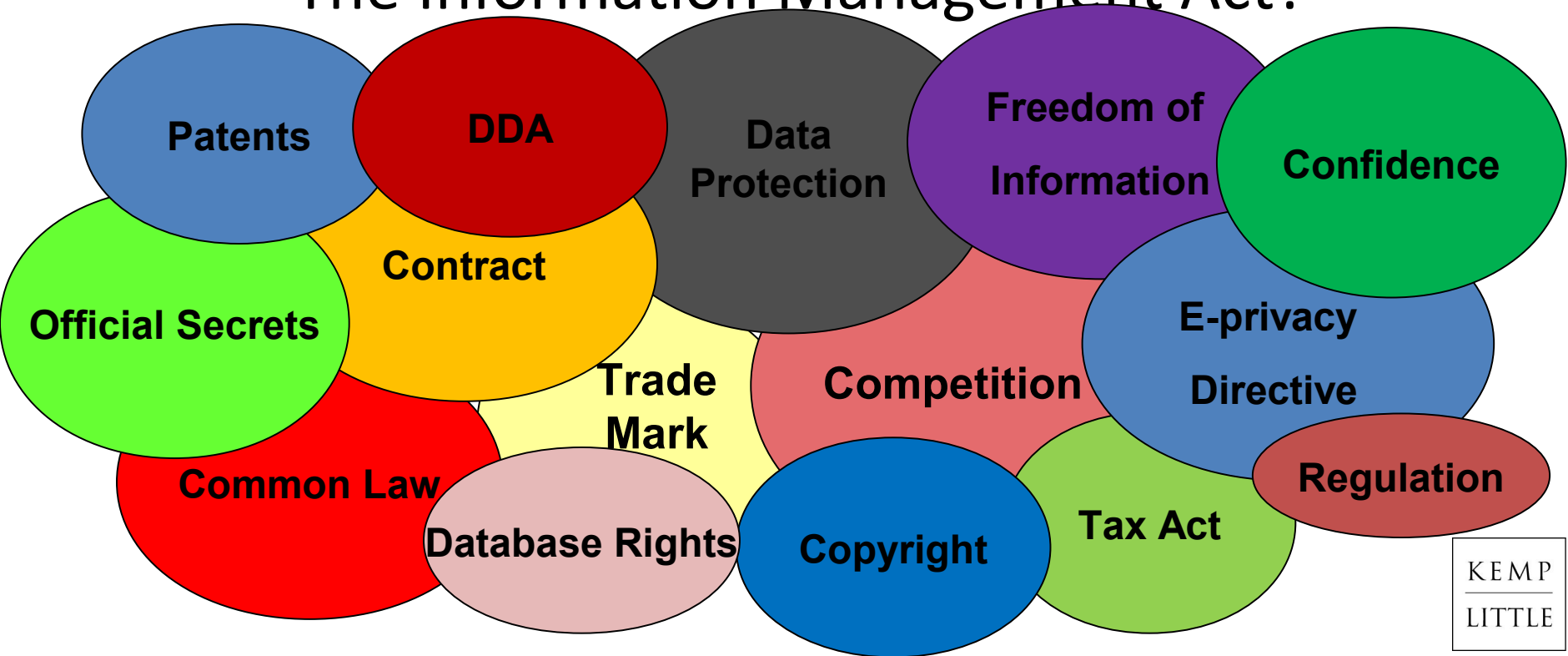
LLP

Information: good, bad and...

- Information is:
 - increasingly available and accessible
 - can be more efficiently and easily stored and used
 - of increasing value and importance
- Increasing number and severity of data losses/thefts
- Increasing media coverage and awareness
- Increasing amounts of law/regulation/fines and litigation
- Bad PR and can lose business
- An issue which is rising up board agendas



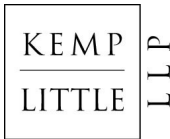
The Information Management Act?





Law and Information Management - Commercial Perspective

1. Security/confidentiality obligations
2. What information can/must be stored
3. Exploitation of information
4. Who has a right to access information
5. Third party dealings – employees, customers, suppliers + intra-group



Security/Confidentiality: Protections (i) Computer Misuse Act 1990

- Unauthorised access to computer material – 2 years + fine
- Unauthorised access with intent to commit or facilitate commission of further offences – 5 years + fine
- Unauthorised modification of computer material – 10 years + fine
 - Interpreted widely – e.g. “guessing a password”
 - Vicarious liability



Security/Confidentiality: Protections (ii) Theft

- Theft of property e.g. laptop but..
- *Oxford v Moss* [1979]
- Engineering student studying at Liverpool University
- Took exam paper but intended to return it
- Only “taking” knowledge of contents
- Not theft of “property” under the Theft Act



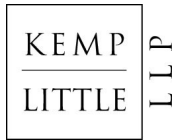
Security/Confidentiality: Protections (iii) Confidentiality

- Common law
- Confidential in nature – “necessary quality of confidence” not in public domain
- Disclosed in circumstance importing an obligation of confidence



"reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence"

- Employee – and ex-employee cases
- Enforceable against the recipient or any subsequent third party recipient of such information, even where such third party had no knowledge of its confidential nature



Security/Confidentiality: Protections (iv) Contract

- Metered access – right to set the agenda
- Imposition of clear security/confidentiality obligations at every stage via contract:
 - Licence/Usage Clauses - set out **only what may be done** in detail – **and exactly what security standards apply** - reserve all other rights
 - Compliance with laws and regulation e.g. DPA
 - Compliance with policies
 - Change management
 - Audit rights
 - Reporting of loss
- If breached - right to terminate and sue for damages
- Can impose other contractual consequences

Security/Confidentiality: Obligations (i) DPA – Principle 7

- Principle 7
“appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”
- Subjective depending on type of business and sensitivity of information
- Organisational measures
- Staff
- Physical security

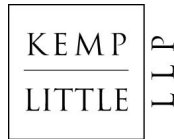
Security/Confidentiality: Obligations (i) DPA – Principle 7

Computer Security

- Not ‘state of the art’ technology - take cost into account. Must be appropriate for the harm that could result and nature of the information.
- Anti-hacking software and procedures
- Encryption of customer data in portable media
- Applicable IT standards “keeping up to date”
- Practical measures and security standards

ISO standards– e.g. ISO 27000 / BS 7799 (BS 10012 – Data Protection)

- Reviewing and set clear internal standards



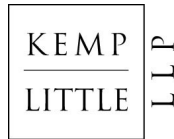
Security/Confidentiality: Obligations (i) DPA – Principle 7

Greater policing and penalties: £500,000

- e.g. - ICO 8 Feb 2011 - Ealing Council and Hounslow Councils fined - unencrypted laptop theft
- **Published** undertaking to the ICO


I hope all organisations that handle personal information will make sure their houses are in order – otherwise they too may have to learn the hard way.”

Following the incident, both councils contacted affected individuals. Both authorities have also put significantly improved policies in place for information security and have agreed to consider an audit by the ICO



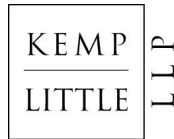
Security/Confidentiality: Obligations (ii) Regulator – e.g. FSA

- FSA Principle 3 – *“A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”*
- FSA Principle 2 – *“A firm must conduct its business with due skill, care and diligence”*
- E.g.s of data security breaches in Financial Services:
 - 2010 Zurich Insurance: £2.275,000 – loss of 46,000 policy details
 - 2009 HSBC (various): £3,185,000 – unencrypted customer details sent in post
 - 2007 Norwich Union: £1,260,000 – telephone customer ID system enabled fraud
 - 2007 Nationwide: £980,000 – poor systems in relation to lost laptop



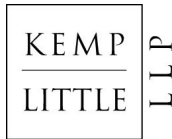
Security/Confidentiality: Obligations (iii) Industry Specific – PCI DSS Rules

- PCI DSS includes 12 requirements for any business that stores, processes or transmits payment card data
- The 12 requirements include:
 - Not to store Sensitive Authentication Data
 - Secure Network
 - Protect Cardholder Data
 - Maintain Vulnerability Management Program
 - Strong Access Control Measures
 - Monitor and Test Network



Legal Recap

- **Generic Legal Protections** - some protection but only useful once the horse has bolted...
- **Legal Security obligations** – generic obligations to keep data secure and some specific obligations
- **Compliance Answer** - No “silver bullet”
 - Take charge of the problem by actively reviewing and assessing the risks
 - Develop clear strategy and policies for managing data
 - Multi-faceted approach:
 - Contractual/legal
 - IT security/solutions
 - Practical policies and procedures
 - Impose the standards/policies via contract on employees, customers, suppliers + intra-group

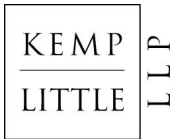


Must have policies

- Comprehensive review of all information and applicable policies:
 - document retention policy
 - document storage policies – e.g. email archiving
 - employee HR/policy
 - communications policy (phone, email, internet etc)
 - privacy policy
 - terms and conditions
 - back-up/disaster recovery policy

“Not having the information you need when you need it leaves you wanting. Not knowing where to look for it leaves you powerless”

Lois Horowitz





Advantage of Policies

- Make it an employee/supplier issue wherever possible:
 - written documents that explains practical day-to-day procedures and rules for use of the data (including communications, storage, passwords, access, home working etc etc)
 - provided to all employees/suppliers who have to sign and comply with them (part of employment / outsourcing contract)
 - will reduce the real risk of a leak occurring
 - will increase chances of compliance with laws and regulation
 - will reduce liability
 - significantly improves PR damage

Policy Tips

- Management buy-in, approval and support
- Write clear and simple user friendly policies
- Identifying the benefits
- Clear objectives
- Include all business areas
- Make policies accessible – Intranet
- Allocate sufficient resources
 - Appoint local department members responsible for implementation
 - Provide training
 - Regular checks and updates
 - Appoint a data loss response team and strategy
- Do not underestimate the task!



Example of a Practical Solution

Problem:

Transfer of employee data to third party supplier - **RISK**

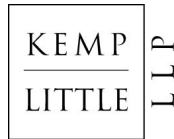
- Potential breach of data protection legislation
- Reputational damage if data is disclosed
- Possibility of employee dissatisfaction due to data loss

Solution:

- Use masking software to hide personal data
- Ensure contract has adequate data security obligations and protections

Result:

- Risk reduced, compliance increased – supplier issue not company problem



Information Management - Strategy

- Identify what to keep
- Keep what is needed – securely and enable its exploitation to the fullest
- Delete what isn't needed
- Increase compliance and business efficiency, reduce risk and cost
- Ensure all contractual/policy terms accurately reflect strategy
- Police your compliance

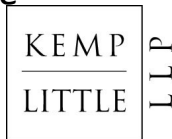


“Information is not knowledge.”

“Everything should be as simple as it is, but not simpler.”

“The hardest thing to understand in the world is the income tax.”

Albert Einstein





Paul Hinton

Commercial technology partner
Kemp Little LLP

paul.hinton@kemplittle.com

Tel. +44 (0) 20 7710 1623

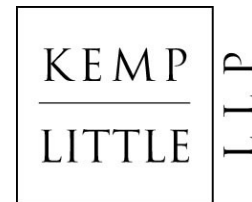


Ivor Drake

Commercial technology solicitor
Kemp Little LLP

ivor.drake@kemplittle.com

Tel. +44 (0) 20 7710 1607



For more information:

www.kemplittle.com