

Confidential Collaboration:

How to manage regulatory compliance & data privacy
while keeping your data safe



Contents

Executive Summary	1
why you should read this White Paper	
Landmark incidents and activities	2
The legal risks of uncontrolled collaboration and information sharing and what to do about them	3
Jurisdictional privacy heat map	5
Critical legal issues	8
Our recommendations for good governance	18

Intralinks

This white paper has been commissioned by Intralinks, a leading global technology provider of beyond the firewall content management and collaboration solutions. Over 99% of the Fortune 1000 use the Intralinks platform to enable the secure and compliant exchange, management and control of documents and content between organizations, many of which operate in highly complex and regulated business sectors. Please visit www.intralinks.com for more information.

For further information please do not hesitate to contact:



Stewart Room
Partner

Tel: +44 (0) 20 7861 4850
Email: stewart.room@ffw.com

Executive Summary

why you should read this White Paper

Business decision makers, including CIOs and CISOs, understand that successful collaboration and information sharing are vital to business success, yet they also carry the responsibility within their organizations to ensure that legal compliance is delivered operationally, on the ground. Collaboration and information sharing activities are already fiercely regulated all over the world but as laws and regulations continue to emerge this presents a driving need for business decision makers to ensure legal compliance.

Organizations that ignore the law affecting collaboration and information sharing are at serious risk of litigation, fines and brand damage.

Organizations need to take a proactive stance on how, where and what information they share and store on cloud services, and under what circumstances, remembering to maintain a focus at all times on the legal and regulatory implications and the threats and risks to their data.

In this White Paper we make recommendations about the steps organizations should take as part of a program to help achieve legal compliance; readers will soon appreciate that many of these steps can only be taken with the involvement and support of CIOs and CISOs.

Why are law makers and regulators treating collaboration and information sharing so seriously?

To help business decision makers understand why law makers and regulators are treating collaboration and information sharing so seriously, we refer to the recent pattern of very high profile news stories about information use, access and sharing, which have garnered international attention.

The events discussed in the table below show that these topics are incredibly important in a political, economic and societal sense, hence why collaboration and information sharing are treated so seriously within the law.



Landmark incidents and activities

Landmark incidents and activities of major political importance that generated global media attention – the reasons why lawmakers and regulators around the world treat information handling so seriously

Event	Impact	Relevance
2007 – Her Majesty's Revenue & Customs (HMRC) loses two unencrypted disks containing personal data on 25 million UK citizens.	One of the world's biggest data loss cases, attracting international press and media attention, undermining public trust and confidence in the Government. UK data protection law is changed as a result, to give the data protection regulator the power to impose fines of up to £500,000 (\$815,000 USD) on organizations that fail to keep personal data safe, secure and confidential.	HMRC was trying to share information with and collaborate with another Government Agency, but the disks were lost in transit. The fall-out of this case means that UK law- and public opinion- now have a low tolerance for unsafe business practices that put personal data at risk of loss or unauthorized access.
2008 – Cybersecurity	The topic of cybersecurity, including "cyber warfare" and "cyber terrorism", percolated in the wider public awareness in 2008 and it has remained a newsworthy hot topic ever since.	It is widely known that cybersecurity issues include espionage issues, whether State-sponsored, criminally motivated, or business-on-business. Like the Phone Hacking Scandal and Hactivism, organizations are reminded that there are external threats to their networks and data.
2010 – Wikileaks releases US diplomatic cables and helicopter gunship footage.	The Wikileaks story has shone an intense international spotlight on the role of the Whistleblower and the vulnerability of organizations to insider disclosures of secret and confidential information.	The "insider threat" is a risk that can be present in any organization. Wikileaks tells organizations that they need to be alert to their confidential information being deliberately disclosed by people who have lawful access to it.
2011 – Hactivism, Anonymous & Lulzsec	The "Hactivist" collectives, Anonymous & Lulzsec, managed to attract intense publicity through their DDOS campaigns aimed at Government bodies, law enforcement agencies and big companies.	Although a DDOS attack is not specifically aimed at obtaining and disclosing confidential information, the actions of Anonymous and Lulzsec drew attention to the fact that organizations are vulnerable to a much wider range of cyber threats, which do not necessarily need massive resources to mount, such as "phishing" and "pharming", which really do pose risks to data.
2012 – Phone Hacking Scandal (including The Leveson Inquiry)	The Phone Hacking Scandal brought an end to the News of the World newspaper, it has put many powerful press people in the dock of the criminal court, and it has caused the UK political establishment acute embarrassment, all in the glare of international press and media attention.	The actions of the News of the World provided a very loud reminder of the fact that data are vulnerable to systematic abuse and crime. Essentially, Phone Hacking was a crime of "pre-texting", or social engineering, against which all organizations in charge of confidential information need to be on their guard.
2013 – Edward Snowden leaks information about the US PRISM program.	Snowden's leaks about the PRISM program and other data collection activities of the US National Security Agency have achieved as much, if not more, press and media attention as the 2010 Wikileaks publications.	This is another reminder of the insider threat to secret and confidential data. Organizations are also reminded that governments are interested in their data.

The legal risks of uncontrolled collaboration and information sharing

and what to do about them

Many organizations are slow to realize the threats posed by ungoverned collaboration and information sharing.

With the evolution and proliferation of collaboration and information sharing tools (from consumer-focused, online document sync and share applications through to social networking sites), improved mobile connectivity, the adoption of agile working practices, and device affordability, users are becoming increasingly self-sufficient and in control of their own IT provisioning.

Essentially, organizations' perimeters are deconstructing. This paradigm shift from organizationally-defined to user-defined information governance means that organizations are losing control of business activity and data.

A loss of control over commercially sensitive or highly regulated information can involve significant legal risk, including:

- Breach of data protection and privacy. Organizations need to be on heightened alert when it comes to the sharing of personal information. The unlawful sharing of personal information can lead to regulatory fines, litigation and brand damage through bad publicity.
- Breach of duty of confidence. Organizations that hold information under a duty of confidence risk litigation and damage to their commercial interests and business relationships if the information is shared in breach of that duty.
- Breach of litigation rules governing the preservation and disclosure of documents and evidence. Most jurisdictions require the parties to litigation to preserve documents and evidence and to give disclosure to the other party. Organizations that do not manage their information properly face court sanctions, increased legal costs and the loss of the case if they do not comply with their obligations.
- Breach of corporate governance rules. All companies need to keep good records of their sales and purchasing activities; listed companies need to be careful about breaching stock market disclosure rules and the risk of insider trading; large companies with market power need to be careful about anti-trust behaviors resulting from the creation of cartels. Failures of good corporate governance around records-keeping and information sharing can put organizations in breach of a myriad of regulations, exposing them to regulatory sanctions and brand damage.

Recommendations to reduce or avoid unacceptable legal risks

In order to reduce or avoid unacceptable legal risks, we recommend that organizations take the following actions:

1. **Adopt a considered position on collaborative working and information sharing.** CIOs and CISOs will understand that safe and secure collaborative working and information sharing requires planning and a methodical approach to the assessment of risk. Ignoring the issues is the speediest route to legal problems.
2. **Be aware of the phenomenon of unofficial "self-procurement" of technology in the work place.** As the "Bring Your Own Device" (BYOD) phenomenon reveals, workers do self-procure IT applications and solutions to facilitate collaborative working and information sharing, often using their personal devices, equipment and online accounts.

Fines for unsafe sharing of information

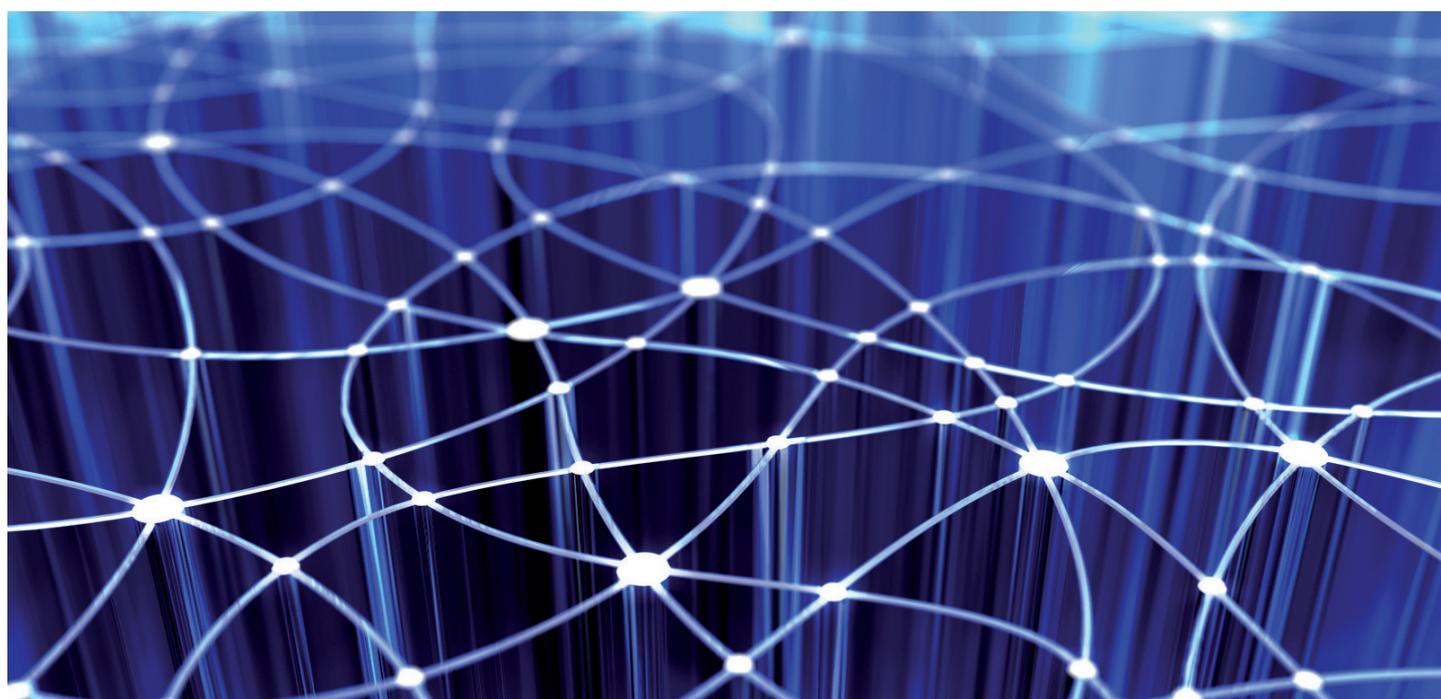
In 2012 the UK Information Commissioner, the regulator for privacy and personal data, fined two public authorities £120,000 (\$190,000 USD) and £80,000 (\$130,000 USD) for sending emails to the wrong recipients. These cases illustrate the risks of using email for collaborative working and information sharing.

3. **When choosing a technology solution for collaborative working and information sharing, focus also on enabling “good governance”, in addition to the technical ease of sharing.** A good platform should enable the organization to track, log and control how information is shared. Bear in mind that email was not designed to offer good governance, and carefully evaluate the quality of the governance offered by new, consumer-type online file sharing applications.
4. **Work with a technology vendor with a proven track record in facilitating and supporting safe and secure collaborative working and information sharing.** A high quality vendor will be able to demonstrate deep experience and sector understanding built up over many years of engagement with enterprise customers, and will have substantial customer support operations in place to help deal with queries and problems.

In other words, organizations need good governance for collaborative working and information sharing. We summarize our recommendations for good governance at the end of this document.

Uncontrolled collaboration and information sharing involves non-legal risks too

Of course, uncontrolled collaborative working and information sharing also pose a variety of non-legal risks. Readers should be aware that the commercial value of an organization’s own Intellectual Property Rights (IPR) may be undermined if they aren’t carefully controlled; indeed it may not be possible to patent an invention if news of its existence leaks to the outside world before the patent is applied for. Productivity and efficiency may also be reduced if appropriate technologies are not provided for collaboration and sharing.



Jurisdictional privacy heat map

Multi-national organizations that appreciate the need to improve their practices for collaboration and information sharing may benefit from an at-a-glance guide that shows the relative strength of a country's legal framework for privacy.

COUNTRY	LEGAL FRAMEWORK FOR PRIVACY	LIKELIHOOD OF REGULATORY FINES AND/OR LITIGATION Readers can assume that countries that treat breaches of law the most seriously provide the "safest" places for location of data, in terms of legal rules preventing unlawful access to data.
AMERICAS		
USA	US takes a sectoral approach to privacy law, with key pieces of legislation for sectors such as financial services and health. Multi-faceted Federal and State legislations for breach disclosure. Active regulators like the FTC are keen to enforce the law through high financial penalties and requirements for compulsory audits. Civil litigation for privacy breaches is a real risk.	Privacy breaches are met with serious punishment in the forms of high regulatory fines and the imposition of compulsory audits. High possibility of harmful civil litigation.
CANADA	Two key pieces of legislation that mirror many aspects of the EU data protection regime, but no risk of regulatory fines. Some risk of civil litigation, but low.	Low risk of adverse proceedings for privacy breaches.
BRAZIL	Some constitutional protections for privacy but no specific data protection law.	Very low risk of adverse proceedings for privacy breaches.
MEXICO	Legislation principally based on EU Data Protection law, with active regulator that has shown an appetite to fine.	Privacy regime still in relative infancy, but regulator has imposed high fines on the financial services sector.

 Strong likelihood of fines and/or litigation

 Possible likelihood of fines and/or litigation

 Low likelihood of fines and/or litigation

COUNTRY	LEGAL FRAMEWORK FOR PRIVACY	LIKELIHOOD OF REGULATORY FINES AND/OR LITIGATION
---------	-----------------------------	--

Readers can assume that countries that treat breaches of law the most seriously provide the “safest” places for location of data, in terms of legal rules preventing unlawful access to data.

EUROPE

UK	Principally based on EU Data Protection and e-Privacy law, with sectoral financial services focus. Breach disclosure rules for sectors like telcos, ISPs, financial services and health. Very active regulator. Litigation starting to appear as a real risk.	Privacy breaches are met with serious punishment in the forms of high regulatory fines. High possibility of harmful civil litigation.
GERMANY	Principally based on EU Data Protection and e-Privacy law, with sectoral financial services focus. Breach disclosure rules apply. Litigation starting to appear as a real risk.	Privacy breaches are met with serious punishment in the forms of high regulatory fines. High possibility of harmful civil litigation.
NETHERLANDS	Principally based on EU Data Protection and e-Privacy law. Breach disclosure rules apply. Low level litigation risks.	Privacy breaches attract a high possibility of regulatory action and are likely to be met with high fines in the medium term.
RUSSIAN FEDERATION	Data protection laws mirror core aspect of EU Data Protection law, with breach disclosure rules. Low level litigation risks.	Possibility that legal regime will mirror that in Europe in the longer term.
SPAIN	Principally based on EU Data Protection and e-Privacy law. Breach disclosure rules apply. Low level litigation risks.	Privacy breaches attract a high possibility of regulatory action and are regularly met with high fines.
SWEDEN	Principally based on EU Data Protection and e-Privacy law. Breach disclosure rules apply. Low level litigation risks.	Privacy breaches do attract regulatory attention and imposition of fines in serious cases, but the impression is given that data protection law is not enforced with the same zeal as in other EU countries.
SWITZERLAND	Principally based on EU Data Protection, with specialized protection for banking secrecy. Low level litigation risks.	Privacy breaches do attract regulatory attention but the impression is given that data protection law is not enforced with the same zeal as in other EU countries.
NORWAY	Principally based on EU Data Protection and e-Privacy law. Breach disclosure rules apply. Low level litigation risks.	Privacy breaches do attract regulatory attention and imposition of fines in serious cases, but the impression is given that data protection law is not enforced with the same zeal as in other EU countries.

COUNTRY	LEGAL FRAMEWORK FOR PRIVACY	LIKELIHOOD OF REGULATORY FINES AND/OR LITIGATION Readers can assume that countries that treat breaches of law the most seriously provide the “safest” places for location of data, in terms of legal rules preventing unlawful access to data.
---------	-----------------------------	--

APAC		
CHINA	Forthcoming legislation that mirrors some aspects of the EU Data Protection legal framework.	Possibility that legal regime will mirror that in Europe in the longer term.
JAPAN	Contained in legislation that mirrors some aspects of the EU Data Protection legal framework.	Possibility that legal regime will mirror that in Europe in the longer term.
HONG KONG	Contained in legislation that mirrors some aspects the EU Data Protection legal framework.	Possibility that legal regime will mirror that in Europe in the longer term.
S.KOREA	Contained in legislation that mirrors some aspects the EU Data Protection legal framework.	Possibility that legal regime will mirror that in Europe in the longer term.
SINGAPORE	Contained in legislation that mirrors some aspects of the EU Data Protection legal framework.	Possibility that legal regime will mirror that in Europe in the longer term.
AUSTRALIA	Currently a limited Federal privacy regime, supplemented by State level data protection laws that mirror some aspects of the EU data protection regime. A major overhaul of the law will come into effect in 2014 however. Some risk of regulatory investigations and litigation, but risks low.	Possibility that legal regime will mirror that in Europe in the longer term.
N.ZEALAND	Legislation similar to the EU Data Protection law, with active regulator, but low risk of fines. Low level litigation risks.	Possibility that legal regime will mirror that in Europe in the longer term.

-  Strong likelihood of fines and/or litigation
-  Possible likelihood of fines and/or litigation
-  Low likelihood of fines and/or litigation

Critical legal issues

Privacy, Security and Confidentiality

The privacy, security and confidentiality of information are critical legal issues that affect organizations all over the world. The recent furor over the US National Security Agency **PRISM program** serves as a timely reminder that these topics can rise to the very top of public and political agendas, with potentially profound implications. Another example from the **UK** is the News Corp. "**Phone Hacking Scandal**", which continues to make the headlines.

Laws have developed the furthest in the data protection field; in both Europe and the United States the processing of personal information by computers and other electronic equipment is highly regulated by legislation such as the **Data Protection Directive in the EU and Health Insurance Portability and Accountability Act (HIPPA), Gramm-Leach-Bliley Act (GLB) and Federal Trade Commission Act (FTC) in the US.**

The "Data Protection Principles"

The data protection principles require data controllers to:

- Process personal data only for specified, legitimate purposes.
- Process the minimum amount of personal data possible.
- Keep personal data accurate and up to date.
- Delete personal data when they are no longer needed.
- Comply with the exercise by individuals of their data protection legal rights, such as the right to be supplied with copies of their information.
- Keep personal data safe, secure and confidential.

Where are Data Safe?

Within the EU, US and similar western economies, the law provides strong guarantees for privacy, security and data protection, so that most organizations can assume that data housed in these jurisdictions is legally protected from unauthorised access and use.

These jurisdictions also have strong legal safeguards against access to data by the State, including by law enforcement bodies, albeit there are no countries that place an absolute embargo on access to data by the State.

In countries such as China and Russia it might be considered that the legal protections against State access to data are lower than those in the west. As a rule of thumb, in countries where the Rule of Law is strongest, i.e., in the EU, the US and other western economies, it is safe to assume that there are legal processes in place that are intended to place limitations and oversight on State level access to data and so these countries are the safest places to locate data, if the organization is concerned about data access by the State.

Data protection law in the EU – regulating Privacy, Security and Confidentiality

European data protection law prescribes a set of mandatory principles for the processing of personal data (information relating to identifiable, living individuals) by “data controllers”.

An organization is considered a data controller if it has responsibility for deciding what happens with personal data. EU law is “omnibus” in nature, which means that it covers all sectors of the economy, unlike the approach in the US, where the legislation focuses on critical areas such as health, financial services, consumer protection and child protection.

The concept of processing is very broadly drawn, covering all aspects of data use from initial collection, through to sharing with others and collaborative working, through to final destruction or deletion. Virtually every business operating in the EU is considered a data controller, either with respect to its employees’ personal data, its customers’ personal data or its contracting partners’ personal data.

Breaches of data protection law are actively enforced by the national data protection regulators. These breaches can trigger complaints and litigation, and can lead to brand and reputation damage. Therefore, it is absolutely vital that all organizations that process personal data understand the principles within the law, how breaches of the law can occur, and what can be done to prevent them.

Quite simply, organizations that do not adopt a considered position on collaborative working and information sharing can easily find themselves in breach of data protection law.

Privacy risk examples

The following examples illustrate the legal risks inherent to collaboration and information sharing. Whether or not these activities are conducted with or without the organization’s knowledge, consent or permission, the responsibility for ensuring legal compliance always rests with the organization.

Example 1: Member of staff decides to share another person’s personal data through the Cloud, without permission

- If a member of staff takes it upon him or herself to share another person’s personal data with a third party through a personal Cloud-based file sharing application, without the consent of their employer (the data controller), they will immediately put their employer in breach of the law.
- The breach of law can be analyzed in many different ways; it will obviously constitute a breach of the security and confidentiality principle, because the personal data are no longer within the control of the employer, hence they are insecure.
- If the server hosting the file sharing application is based outside of Europe in an “unsafe” country, or if personal data are accessible in an unsafe country (i.e. the country does not have national legislation that meets EU data protection law standards)—for example, if the data controller has not utilized one of the approved EU mechanisms for the safe transfer of data (“the data export rule”) such as the US Safe Harbor scheme, the employer will also be in breach of the data export rule.

The security and confidentiality principle within EU data protection law

The EU Data Protection Directive requires data controllers to implement appropriate technical and organizational measures to protect personal data from security breaches and breaches of confidentiality. This legal duty to be secure covers all forms of threats and risks to personal data, including those arising through unsafe sharing and collaboration.

- Because the data exist as copies in the Cloud, the employer will also be in breach of the data minimization rule (which says that organizations should limit the amount of personal data that are processed to the smallest amount possible), as the data will have proliferated.
- Because the data are beyond the company's control, it will not be able to enforce a deletion policy, prevent further dissemination, or describe the data's whereabouts when receiving a request for information from the person whose personal data has been shared, let alone provide satisfactory answers to a formal regulatory inquiry.
- The European data protection regulators would treat this as a very serious case. In major EU economies such as the UK, Germany, France, Italy and Spain, the regulators would consider imposing a fine.

Privacy law requires full information governance

In the case of *L v. Finland*, the European Court of Human Rights found that it constituted a breach of European privacy law for a hospital to operate a computer system that did not retain long-term logs of access to data.

Data access and use must be fully auditable.

Example 2: Employer allows employee to use their own Cloud-based "sync-and-share" account

- In Example 1 the member of staff used a Cloud-based sync-and-share application without their employer's knowledge or consent. If the employer allows the employee to use their personal Cloud account, it will still be in breach of data protection laws if the employer has lost full or partial control over the data or cannot fully audit what has happened to the data in terms of use, access or sharing.
- The critical takeaway for organizations is that compliance with EU data protection laws requires the use of technology platforms that keep the organization in full control of data.

Example 3: Employer provisions a Cloud-based "sync-and-share" account for the workplace

- In Examples 1 and 2, files were shared through the employee's personal Cloud-based sync-and-share application. If the employer supplies an account for use in the workplace, it will have much greater visibility and control over the data.
- That said, if the application does not enable full Information Governance, such as auditing of access or alterations to the data, or the setting of access rights and privileges, the employer will still be in breach of law.

Choosing a Cloud service provider

So, if an organization is going to use a Cloud-based system for collaborative working and information sharing, what must it look for to be legally compliant? Reflecting official guidance on Cloud Computing published by the EU data protection regulators in July 2012, an organization should:

1. Ensure that it puts in place a written contract with the Cloud service provider, under which the service provider promises to comply fully with data protection law at all times.
2. Carry out a risk assessment to understand any vulnerability caused by putting data into the Cloud, and the potential harm that will be caused if there is a security breach or other form of unlawful activity.
3. Satisfy itself that the service provider has implemented sufficient technical and organizational security measures to protect personal data, and to achieve the security objectives of availability, confidentiality and integrity of data.
4. Ensure that the service itself keeps the organization in control over the data, particularly over access rights and privileges.
5. Ensure that the service itself permits the logging and auditing of data access and use.

Working with reliable partners – due diligence on their reliability and trustworthiness

Any third party organization that handles personal data in order to provide support— say hosting support, rack space or Cloud services— is known as a “data processor”. In other words, any organization that provides a technology platform for collaborative working and information sharing will be a data processor, if personal data pass through the platform.

An organization’s relationship with its data processors is highly regulated by EU data protection law, one of the rules being that there needs to be a contract in place under which the service provider promises to comply fully with data protection law at all times. Additionally, the law states that organizations should work only with reliable and trustworthy data processors, which requires organizations to carry out appropriate pre- and post-contractual due diligence.

Types of due diligence

Obviously, due diligence can take many forms, including formal onsite audits and inspections, but where the service is Cloud-based and where the service provider’s offices, data centers and equipment may be overseas the feasibility of onsite audits and inspections is very low.

Therefore, in most situations due diligence will take the form of research and inquiries into: the service provider’s history, its track record and experience (including any special sector experience, say for financial services, pharmaceuticals or manufacturing); the nature of its systems and operations for security; the holding of any relevant accreditations (such as ISO 27001); the nature, quality and availability of support services and the presence of “people on the ground” who can help to solve problems; the geographical location of its equipment and servers that are used to provide the service (the availability of EU-based equipment and servers makes compliance easier); the extent to which its services support the underlying objective of good data protection – and so on.

Assessing the quality of the service provider’s technology forms part of due diligence

Of course, it is recognized that long histories, good track records, in-depth sector experience and physical location cannot provide absolute guarantees that a service provider is a good data processor, but when it comes to issues of due diligence, these things do matter and they have real legal significance.

The key point for organizations is simply this: in addition to assessing the extent to which the functionality of the platform supports full Information Governance and security, they should also look beyond the technology itself. Data protection legal compliance in the EU needs not only good technologies, but good organizations supplying them.

College fined \$400,000 USD for not carrying out HIPAA security risk assessments

Idaho State University failed to conduct proper security risk assessments. As a result, ePHI stored on their servers were left vulnerable to unlawful access, loss and damage. Idaho was forced to settle the regulatory action by paying a \$400,000 USD fine. The regulator concluded:

“Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program ... Proper security measures and policies help mitigate potential risk to patient information.”

<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement-press-release.html.html>

The state of technological development - what functionality should we look for?

Data security rules require organizations to keep abreast of technological developments and to take account of what is on the market when they devise their strategies for data processing. In other words, the law adopts the default position that the technology estate must be kept up to date with advances in technological development. This is known as "having regard to the state of technological development".

For example, the need to have regard to the state of technological development provides the foundation for concluding that as a matter of law encryption should be applied to portable computers and storage media that hold personal data; firewalls and anti-malware need to be deployed; access to and use of computers and data should be logged - etc.

GLB Act official advice covers collaborative working and information sharing

The FTC has published official advice that makes it clear that organizations subject to the GLB Act need to take control of collaborative working and information sharing:

"...Take steps to ensure the secure transmission of customer information."

" ... Develop policies for employees who telecommute ... consider whether or how employees should be allowed to keep or access customer data at home."

"... monitor both in- and out-bound transfers of information for indications of a compromise"

<http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule>

Examples of good functionality

Therefore, when an organization adopts a third party application for collaborative working and information sharing, it needs to look very closely at the functionality of the technology to determine whether it satisfies the legal obligation to have regard to the state of technological development. The state of technological development includes:

- Functionality that encrypts data at rest or in transit.
- Functionality that enables users to set confidentiality levels to files that are to be shared.
- Functionality that enables the setting of "information barriers" between files and users.

Using Digital Rights Management technologies

We recommend that organizations look out for innovative deployment of Digital Rights Management (DRM) technologies. DRM can be applied to files, to "tether" them to the organization even after they have been shared. By reference to data and time stamps the ability to access the file can be set to expire at a set point in time, effectively unwinding the sharing of the files after the event.

Using DRM in this manner puts this kind of functionality within the state of technological development, and as a matter of law organizations need to consider whether the nature of their data is such that DRM is necessary.

It is also important to note that DRM takes advantage of encryption technologies; the significance of this point lies in the fact that encryption is the only technology that is universally accepted within EU legislation, regulatory guidance, and enforcement actions, as constituting legal compliance with the requirement to apply appropriate technological security controls.

Fines for non-compliance

European data protection regulators are more willing than ever to impose fines when the security or confidentiality of personal data is put at risk through unsafe business practices.

In 2012 the UK Information Commissioner imposed fines on 22 organizations for various kinds of security breaches, a number of which were for unlawful sharing of data as a result of accidental dissemination (by email, fax and post). Google has also been on the receiving end of fines for unlawfully gathering communications data via its Streetview cars (€145,000 [\$190,000 USD] in Germany, €150,000 [\$200,000 USD] in Belgium, €100,000 [\$132,000] in France).

Privacy and security legislation in the US - a strong focus on critical sectors

The United States has not adopted an EU-style omnibus data protection law. However, there are a number of pieces of important Federal legislation that focus on, or have been interpreted to cover, much of the same ground as EU law.

Federal Trade Commission Act ("FTC Act")

The Federal Trade Commission (FTC) has used section 5 of the FTC Act to build a regulatory framework for privacy and security. Section 5 makes it unlawful for a business to engage in deceptive or unfair trade practices. The FTC takes the view that a company has committed a deceptive practice if it misrepresents the level of its security, and has committed an unfair practice if it fails to implement "reasonable procedures" to protect personal information.

So, for example, a company that publishes a statement such as a website privacy policy promising to properly protect customer information from security breaches will be found guilty of both deceptive and unfair practices if it does not maintain control of collaborative working and sharing. Examples 1, 2 and 3 described earlier in this White Paper could easily constitute breaches of the FTC Act.

The FTC has the power to impose massive fines for deceptive and unfair practices and to require substantive organizational change in the business, overseen by long term independent audits. For example, in the CBR Systems case (Jan. 2013), CBR was required to agree to a 20-year independent audit plan because it failed to encrypt back-up tapes containing financial and medical information that were being transported between buildings.

In the Path Inc. case (Feb. 2013), Path had to pay the FTC \$800,000 USD to settle charges that it facilitated the online sharing of children's data without parental consent, in breach of the Children Online Privacy Protection Act.

HTC America - unsafe technology

Despite saying in a user manual that third parties would not be able to access information on handsets without permission, HTC's smartphone software contained coding errors that rendered user data vulnerable to security breaches.

The FTC concluded that HTC breached the FTC Act. To settle the case HTC had to agree to a 20-year process of independent audit.

Gramm-Leach-Bliley Act ("GLB Act")

The GLB Act regulates financial institutions (banks, securities firms, insurance companies), as well as companies providing financial products and services to consumers.

The Act requires these organizations to comply with the Financial Privacy Rule and the Safeguard Rule, in order to protect customer information.

The Financial Privacy Rule requires these organizations to give notice to consumers explaining who their data will be shared with, while the Safeguard Rule requires them to design, implement and maintain safeguards to protect the confidentiality and integrity of personal consumer information. Examples 1, 2 and 3 above can easily constitute breaches of the GLB Act.

The GLB Act is actively enforced by the FTC, which can impose fines and order behavioral changes for breaches of the Privacy

and Safeguard Rules. For example, in July 2012 the FTC charged Franklin's Budget Car Sales Inc. with being in breach of the Act, because Franklin's allowed its employees to share sensitive customer data over P2P file sharing networks.

Health Insurance Portability and Accountability Act ("HIPAA")

HIPAA places a legal obligation on health care providers, health plans, pharmacies – and organizations providing supporting data analysis and processing services – to implement and maintain appropriate technical and organizational measures to ensure the confidentiality, integrity and availability of electronic protected health information ("ePHI").

Critically, the organizations regulated by HIPAA must carry out risk assessments to understand the vulnerabilities to ePHI, which include examining the risks posed by unsafe processing of ePHI. Examples 1, 2 and 3 could easily constitute breaches of HIPAA.

Breaches of HIPAA can lead to the imposition of massive fines. For example, in Nov. 2012 the Alaska Department of Health and Human Services was forced to pay a fine of \$1,700,000 USD to settle regulatory proceedings arising from its failure to conduct adequate security risk assessments, encrypt portable media containing ePHI, and carry out adequate security risk awareness training in the work place.

Other US legislation

There are many other examples of legislation in the United States that mandate organizations to implement appropriate systems and operations to ensure the security of sensitive data at a Federal and State level, such as the Federal Information Security Management Act or the Massachusetts Data Protection Law.

The common theme across all these legislations is that organizations controlling sensitive data should carry out risk assessments to identify threats and vulnerabilities, and then implement appropriate controls to mitigate and manage them.

These need to extend beyond technological security measures to written processes, policies and procedures, staff awareness and training. An organization that fails to address collaborative working and information sharing, holistically and maturely, will be at risk not only of security breaches, but serious legal non-compliance.

However, many organizations are still burying their heads in the sand, or have decided to gamble that they will never get caught. Organizations with these mentalities need to be aware that the law is already building mechanisms that will catch them out.

Breach disclosure laws

The idea behind breach disclosure laws is that if an organization suffers a serious security breach it shall be required to "come clean" and notify the victims and / or official bodies (regulators, or often State Attorneys in the US).

The thinking here is that transparency after failure can help to mitigate harm, loss and damage. The belief is also that the fear of transparency will incentivize organizations to take privacy, security and confidentiality more seriously, to avoid the brand and reputational damage that can follow a high publicity security breach.

Breach disclosure legislation first emerged in the US, in California in 2003. Since then, most US States have adopted their own legislation. At the Federal level it is widely accepted that HIPAA, GLB Act and FTC Act require breach disclosure.

Breach disclosure is not confined to the US. Canada, Australia, the EU and many other jurisdictions have followed the US approach.

Therefore, if an organization does not adopt safe technology, systems and operations for collaborative working and information sharing and a security breach occurs, there is a significant probability that the law will require them to "come clean", with all the consequences that follow.

In the UK, for example, the Information Commissioner (the regulator for data protection) has issued regulatory guidance in which he sets out the situations when he will expect an organization to report personal data breaches to his office. Germany has passed legislation to mandate breach disclosure in all cases where financial data is involved. All across Europe, telcos and ISPs are subject to a mandatory breach disclosure obligation. Forthcoming amendments to the EU data protection regime will make breach disclosure compulsory all across the EU for all parts of the economy.

Other laws that require safe collaborative working and information sharing

There are many other reasons why the law requires organizations to take control of collaborative working and information sharing:

Litigation - preservation and disclosure of evidence and documents	
Requirements:	Risks and consequences:
<p>A key principle of litigation in many jurisdictions is that the parties to a dispute should (1) preserve evidence and documents and (2) disclose evidence and documents to one another as the litigation progresses.</p> <p>This “cards up” approach to litigation is central to the administration of justice and fairness, hence why the courts treat it so seriously.</p>	<p>If a party to litigation is not in control of collaborative working and information sharing, it risks breaching its obligations to preserve and disclose evidence and documents.</p> <p>Consequences for a litigant in default include:</p> <ul style="list-style-type: none"> ▪ Being found in contempt of court ▪ Having judgment entered against it ▪ Damaging its case, because critical evidence cannot be found or presented at court <p>Organizations also need to reflect on the cost of complying with litigation preservation and disclosure rules. As electronic data grows and proliferates within organizations, the cost of “e-discovery” increases. The cost of e-discovery increases if the organization is not in control of its information. A lack of control over collaborative working and information sharing can have massive impacts for e-discovery.</p>

Regulatory disclosures – delivering evidence and documents to supervisory bodies

Requirements:

Many sectors of the economy are highly regulated by independent supervisory bodies, such as financial services (SEC in US, FCA in UK, BaFin in Germany), electronic communications (FCA in US, Ofcom in UK, BNetzA in Germany) and pharmaceuticals (FDA in US, MHRA in UK, BfArM in Germany), as are key economic issues, such as anti-trust and competition (DoJ in US, European Commission in EU) and data privacy (FTC in US, ICO in UK, BFDI in Germany).

In these critical areas, the regulators and supervisory bodies all have wide-ranging legal powers to require organizations to disclose information, often at very short notice.

Risks and consequences:

Organizations that do not comply fully with their regulatory disclosure obligations put themselves at risk of administrative sanctions (such as fines and enforcement notices), criminal proceedings in very serious cases and— where they are licensed—perhaps even the suspension or revocation of their license.

There are two principal scenarios where uncontrolled collaborative working and information sharing can impact an organization’s ability to comply with its regulatory disclosure obligations. First, the organization may not be able to provide complete answers about how its officers and employees have conducted their business, and second, it may not be able to provide all of the documents sought.



Maintenance of information barriers	
<p>Requirements:</p> <p>There are many circumstances where the law imposes obligations on organizations to maintain information barriers to prevent unlawful information sharing. Notable examples include:</p> <ul style="list-style-type: none"> ▪ Anti-trust / competition law – unlawful cartel practice can occur when market operators act in concert, for example on the supply of products and services, or pricing. Inferences of cartels can be drawn from evidence of sharing of certain kinds of information, such as business plans and price lists. Large organizations that are intent on joint ventures need to be careful that they do not breach competition law through uncontrolled information sharing. ▪ Stock market rules – listing and financial services rules place strict obligations on how sensitive business information is handled and when it should be disclosed to the market, to prevent market distortions and insider trading. For example, financial results and major restructuring announcements (takeovers and mergers) need to be reported to the markets and to the public in a controlled fashion, and steps must always be taken to prevent “tipping” – the unlawful sharing of sensitive business information. ▪ Confidentiality law – many businesses will be used to signing Non-Disclosure Agreements (NDAs), which are designed to protect confidential information from misuse or unlawfulness disclosure. In business situations, obligations of confidentiality arise routinely by virtue of the nature of contractual arrangements. Uncontrolled information sharing and collaborative working puts organizations at risk of breaching duties of confidence. 	<p>Risks and consequences:</p> <p>Anti-trust / anti-competitive behaviors and insider trading stand out as two of the most serious corporate behavioral problems, which can lead to massive financial penalties in the forms of fines and criminal prosecutions.</p> <p>Breaches of contractual duties of confidentiality are regularly litigated, at considerable cost, with damages being awarded against the party in breach.</p>
Corporate governance	
<p>Requirements:</p> <p>Corporate governance rules require companies to keep proper records of their transactions and their activities; to address operational risk issues, such as the security of their IT systems and data; and to be fully auditable.</p> <p>Uncontrolled collaborative working and information sharing can put the organization in fundamental breach of its corporate governance obligations.</p>	<p>Risks and consequences:</p> <p>Since Anderson, Enron and WorldCom, the law has treated corporate governance very seriously. If a business cannot account fully for its activities— an obvious risk if the organization is not in complete control of its information— problems can be identified during audit, and in the most serious cases can escalate to strong regulatory action, including fines and even criminal prosecution of directors.</p>

Our recommendations

for good governance

Uncontrolled collaborative working and information sharing can lead to very serious legal problems, so we recommend the adoption of “good governance”.

The following steps should rapidly improve organizations' legal compliance and reduce the risk of unwanted legal consequences:

1. Identify incidents of collaborative working and information sharing in the workplace, the purposes for which the collaboration and sharing takes place, and the tools that are used.
2. Carry out a risk assessment to measure the nature and likelihood of harm that could be caused to data and to third parties (individuals and other organizations) through the collaboration and sharing, including potential legal consequences. Isolate high risk use cases and processes.
3. Take decisions on improvements and changes.
4. Record your key positions in a written “system” of operational rules, then embed them into the organization through training and raising awareness.
5. If you plan to use a third party service provider to support your system, carry out appropriate due diligence and put in place an appropriate written contract.

Recommendations for your technology strategy

Regarding your technology strategy, we make the following recommendations:

1. The use that is made of the technology must be fully auditable, so as to enable the organization to know who accessed data, when they accessed it and what they did with it.
2. Look for technology that requires a minimal amount of behavioral change within the workplace; it should be simple and easy to use and fit for purpose – remember that part of the reason why people “self-procure” is because what is provided for them isn't what they want or need!
3. The technology should enable the user to easily apply readily understandable levels of security to files based on how sensitive they are, and should include fine-grained, customizable access rights and privileges.
4. The technology should facilitate the sharing of files in their native file format, which removes the risk of integrity loss in format conversion.
5. The technology should allow for the creation of individual “work streams”, to help implement information barriers and support access rights and privileges.
6. Look for innovative uses of DRM and encryption, especially in the area of “tethering”, so that access rights and privileges can be time limited and removed, even after information has been shared.
7. The technology should maintain encryption of data at rest,

with high levels of transport encryption, ideally with individual encryption keys for individual files.

Regarding technology vendors:

1. Look for ones with pedigree, track record and industry experience, with key industry accreditations and references.
2. Look for ones which provide support to external parties, not just paying customers, as this will remove some of the operational load of successful and safe collaborative working and information sharing between your organization, its extended supply chain and other third parties.
3. Look for ones that are willing to give their customers access to their premises for security auditing purposes. This kind of access will help you satisfy your due diligence obligations as they apply to your service providers.

And remember – the functionality must be about more than just sharing; it is safe, secure, controlled and auditable sharing that the law seeks!

About FFW

Clients choose to work with us because we provide exceptional lawyers with industry expertise. Our strong commercial knowledge of their businesses enables us to work with them to maximise their market opportunities. They value our flexible approach to teamwork and that we will shape our structures and way of working to meet their specific needs.

Our commercial attitude, combined with our empowering and down-to earth style, means you can trust us to provide you with the best possible legal solutions.

We are acknowledged as leading experts in sectors such as technology media & telecommunications, hotels retail & leisure as well as for our public sector work.

Clients include listed and unlisted companies, multinationals, financial institutions, professional partnerships, trade associations and Government departments. We have 151 partners, over 225 other lawyers and nearly 300 support staff across offices in Brussels, Hamburg, London, Manchester, Munich, Palo Alto, Paris and Shanghai. We also have an exclusive relationship with Italian law firm, La Scala, and affiliate firms across the world.

Our main areas of practice are corporate, IP, technology and outsourcing and regulatory law. We also have leading expertise in areas such as banking and finance, data protection and privacy, financial services, inward investment, real estate, dispute resolution, personal injury and medical negligence.