
Data is the new oil
Privacy is the new green
Unlocking value & Controlling risk
Mind Your! Privacy
Data Science Protected

Data Science Protected

Privacy is the new green

www.MindYourPrivacy.com

Any new business asset…

Data is the new Oil, it's being refined. The initial wave of the Big Data revolution was about processing massive data inputs to render new insights about markets and customers. The next wave is more targeted, stitching data together, putting it to work. It's being scaled against goals. Internal processes and policies are being crafted to make the most out of it.

… will challenge the status quo of your organization and push towards new boundaries of excellence.

Focus on security measures and data integrity.

Privacy is the new Green. Marketers and Agencies erect technology stacks to identify and track customer journeys across screens and beyond the Web to move offline, using the Internet of Things (IoT). The data is supporting more human and personal interactions. Ultimately, companies are becoming the custodians of personal information as data is coming from the customer to serve the customer, supporting the very companies' growth strategies.

With great power comes great responsibility

Yet the protection of data and information is left to a series of unaligned and uncoordinated processes that leave gaps, which increasingly provoke security breaches. Third parties with malicious intentions are increasingly exploiting this lack of stewardship in data governance, harming your customers and your very own organization through unauthorized access to your information assets.

The **security** of any data asset requires a clear view of the data life cycle

Data life cycles to support analytics have been around for years.

Data life cycles to support information security measures & evolving legislation remain scarce.

Mind Your Privacy focuses on developing and supporting those data flows, preventing internal and external menaces.

By controlling data flows, menaces are identified and prevented, providing you with the tools to increase data quality. Could you protect your house without knowing how many doors and windows it has? Or ignoring their sizes?

Data and Information security incidents make companies vulnerable to a variety of risks such as reputational damage, loss of consumer trust, business disruption, fines, legal claims and, of course, disclosure of sensitive competitive information.

Are you ready to protect your data assets?

Defining data life cycles allows you to regain control over key issues by understanding

- **How data is collected** and if consent is aligned with customer expectations;
- **Who has access** to the data within and outside your company;
- **Which type of supplier** due diligence is needed;
- **How to control** and validate suppliers;
- **How to validate** employees accesses and manage their respective authorizations.

According to our experience third party networks are overlapping and interconnecting themselves at various stages of the data life cycle. As a result the exact data flows are not as transparent and clear cut as one might think.

Suffering a data security incident, does this apply to me?

Information security issues are more common than one would think. It explains the recent interest of lawmakers in regulating data breaches. Data security incidents can:

- **Occur for a variety of reasons:** ranging from a simple human mistake, which occurs in 80% of cases, to process failures and, malicious or not, hacking activities;
- **Happen in different ways:** from unencrypted memory sticks to misplaced laptops, lost or accessed by the wrong recipient, to unhappy employees or subcontractors that gets access to confidential information, using it maliciously;
- **Provoke disparate effects:** from compromising highly sensitive commercial information to reveling customers', prospects' or employees' personal data.

10 questions you should ask yourself:

1. Who are your company's Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO)? Does **everybody** know?
2. Who is the **lead** director on information security and is that position informal or formal? Is this part of the Audit Committee's annual work plan?
3. Who is most likely to want access to your company's systems? What level of sophistication, geographic scope and motives (e.g. economic/embezzlement, identity theft, trade secret theft) may these **adversaries** have?
4. Does your company have an **incident response plan**? Has your company identified relevant internal and external (such as technical, legal, public relations) core team members? Has your company set up liaisons with law enforcement authorities?
5. What are your bring-your-own-device (**BYOD**) protocols? Is your company a BYOD environment?
6. Does your company have a clear view on **data flows**? Which information security functions do your contractors provide? What is the level of assurance in the **integrity** of those contractors? How is the company assured that third-party solutions, including software, are free of issues and include indemnification for potential flaws?
7. Has your company assessed the **internal threat**? Does your company monitor internal networks for inappropriate file access or sharing?
8. Does your company actively manage both **physical** and cyber **security**?
9. How does your company interact with suppliers, customers and partners? To which extent does your company provide "**downstream**" products that, if compromised or misused, would affect the company?
10. Are you **training** your staff with a tailored continuous program?

10 tips for a proactive risk reduction:

1. Carry out Risk Assessments regarding data and information to define which level of Governance is required to protect your information assets.
2. Review data access protocols: third parties, suppliers and staff.
3. Review legal retention periods: don't hold on to data you shouldn´t have.
4. Review data life cycles to ensure inaccurate or outdated data is destroyed.
5. Review data transfer protocols, such as encryption and in/out registries, to ensure control and safety.
6. Review backup policies.
7. Put in place a data security incident plan.
8. Clarify your notification protocols in response to data and information security incidents.
9. Ensure home working and/or BYOD policies are consistent with security protocols.
10. Implement training programs for your staff.

Prevention is more cost-effective than any cure.

Mind Your Privacy can help your organization

Mind Your Privacy has developed a unique methodology to help companies define, establish and measure Data Governance Programs. This allows them to create Information Security Systems that properly protect data and information assets.

A Data Governance Program is a **strategy** to ensure **compliance, security** and **data quality** of your information assets. The program's evolution is monitored through organized and planned **performance metrics** to ensure data assets are consistent through rules and standards driven from **policies** executed by **people.**

Why **Mind Your Privacy**?

- Our service offering can be rolled-out through your entire organization or **tailored** for concrete, potentially risky, business areas.
- We offer a **multi-skilled team**.
- Our **experience** related to privacy and security emanates from highly regulated business sectors.
- Our methodology is **based upon EU rules and best practices, fully customizable** to your needs.
- **Practical** and business friendly questionnaires, structured by function and business will help everyone involved to focus on the current status.
- **Fixed price**, established for each company according to review required.

Our multi-skilled team covers all possible scenarios regarding data governance from analytics to compliance.

Mind Your Privacy provides **business solutions**, not business prevention.

Our European rules based expertise and highest best practices standards deliver an **independent view of risks** affecting your company.

Why should **your organization** care?

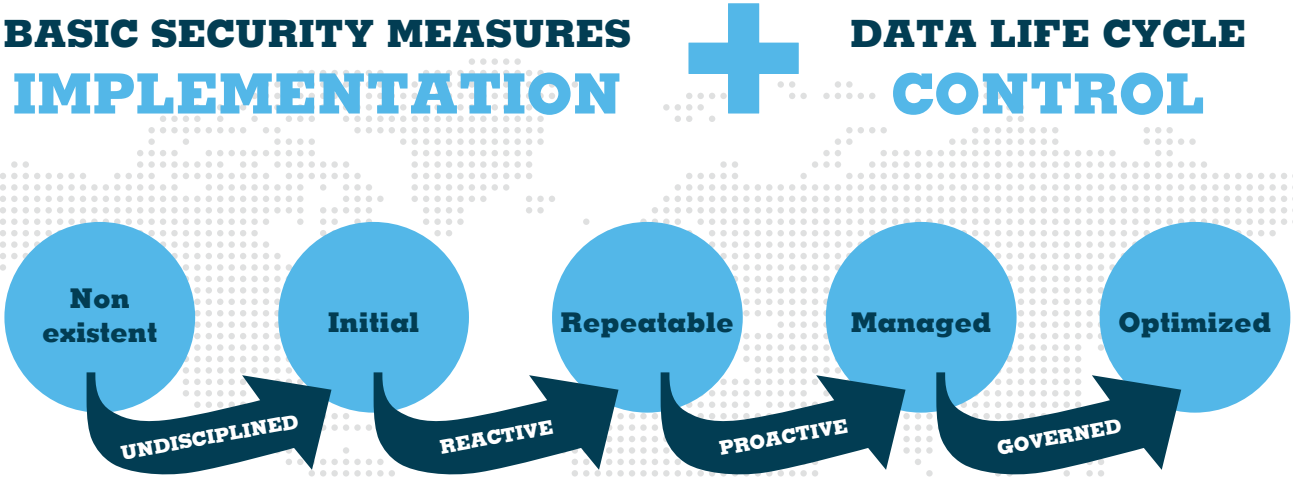
Following increased reporting of business security incidents, privacy compliance, data and information security has become a board level issue. No one wants to deal with a major security incident damaging your company's reputation and exposing it to expensive fines.

COUNTING THE COST OF A SECURITY BREACH	
£ 450-850k	Average cost to large organization 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

How does **Mind Your Privacy** work?

Our approach to instituting comprehensive **Data Governance Programs** fitting your needs, starts with understanding where your company is in our COBIT-based maturity model:



Compliance requires an integral control program of data life cycles, not just tools!

Starting from the establishment of a point of origin, through an audit, defining the current risk and related priorities, **Mind Your Privacy** delivers a roadmap including clear action points and achievable goals.

This **detailed high-level strategic roadmap** can then be implemented by you or with our help. You decide.

While main operational functions are common to most businesses, **Mind Your Privacy** fully understands that each organization is uniquely structured. The key to an effective audit resides in adapting to the specificities inherent to your organization. Initial specifically tailored questionnaires will allows us to understand your business, guaranteeing the audit is tailored to your unique needs.

Once a first clear picture emerges of how your organization or a specific department is set-up, we will work on-site through established meetings and audit events, carried out by a full-time dedicated team. This will allow us to **properly evaluate the current situation**.

An evaluation of the current situation is created from the obtained information in order to build the most **adequate and realistic roadmap** to be implemented by you or with our help. The implementation as such needs then to be specifically priced.

BUSINESS CASE

BACKGROUND AND ISSUES

Mind Your Privacy was asked to verify the data flows emanating to and from the Digital Marketing Services of a multinational retailer. The client used a centralized CRM system, amongst other tools. Data was collected through its subsidiaries and transferred to HQ.

MIND YOUR PRIVACY INVOLVEMENT

Through preliminary questionnaires, basic information was collected to prepare for two on-site days of interviews with key stakeholders.

MIND YOUR PRIVACY FINDINGS

From a security perspective, **Mind Your Privacy** noted that the current control systems between HQ and its subsidiaries were highly insufficient:

- Unsupervised processed data by digital agencies in most subsidiary countries and **inexistent or poorly respected processes**. Hence, the way data was collected, stored and deleted was obviously beyond HQ's control while clearly engaging the central entities' legal responsibility. This situation presented a huge **risk** for a very well known global brand in terms of **possible fines** not to mention huge **reputational issues**.
- Social Media profiles where managed in an uncoordinated fashion, providing a highly **unclear view of data life cycles** through that channel and **risking brand integrity**.
- **No process to recover data** from old customers existed nor did a process to delete such data. This provoked a **massive out-to-date data** bottle-neck, stored without any specific plan of action, adding an unnecessary risk of possible faulty use of said data, possibly damaging this company's brand image.

What our **clients says** about us:

We have knocked on the doors of big international consultancies and of renowned international law firms. Only Mind Your Privacy delivers a clear picture of our current situation and actionable suggestions to improve our data governance and deliver a better understanding of our road to increased Privacy for our customers. The services offered are state-of-art, innovative and highly flexible. We look forward to a long lasting and fruitful collaboration.

Some of our clients are:

IBM NOKIA Bupa

MUFG Bank of Tokyo-Mitsubishi UFJ NATIONAL GEOGRAPHIC PSA

Some of **our services** are:

- Risk assessments
- Cloud procurement advice
- Analytics
- Day-to-day privacy compliance
- Security incident management
- Tailored training to staff, managers or directors
- Helping organizations get ready for data governance changes across the European market

Mind Your! Privacy

Founders

René Dechamps

Aurélie Pols

María Gómez Moriano

Mind Your! Privacy

SPAIN • GERMANY
AUSTRIA • SWITZERLAND
UK • THE NETHERLANDS
SCANDINAVIA

www.MindYourPrivacy.com

Headquarters: Madrid

René Dechamps • **CEO**
rene@mindyourprivacy.com

Aurélie Pols • **Chief Visionary Officer**
aurelie@mindyourprivacy.com

María Gómez Moriano • **Director**
maria@mindyourprivacy.com

Privacy
is the new green