Not all data is created equal

By Aurélie Pols

Following on from our Top 7 Trends in Pharma Marketing for 2015 post we it is clear that the pharma marketing trends we expect to transform the healthcare sector are easier said than done. Aurélie Pols from Mind Your Privacy has written this guest blog to talk about the first steps you need to take when considering data, security, and privacy.

In 2002 statistician Andrew Pole was asked by his colleagues in the marketing department at Target **"*If we wanted to figure out if a customer is pregnant, even if she didn't know, can you do that?*"** Little did he know that by exploring customers' shopping behaviour and merging data to predict the potential pregnancy state of an individual, he would be crossing some important legal boundaries.

Following a data breach, Target found themselves in the news headlines, however little to nothing has been written about the creation of a health state variable – being pregnant or not – based on shopping behaviour.

Read the Target case study in full via the NY Times

As former counsellor of the CNIL President for Advanced Studies, Development and Cooperation, the French Data Protection Agency, Marie Georges stated at the Madrid Google Cathedra in 2014 "*You can't use created sensitive data without consent. The Target case would not have been possible in Europe*".

Europe talks about Data Protection: the riskier the type of data used, the more protected the data should be, thus the higher the accompanying information security measures should be. Typically, a health state like pregnancy requires careful care when being used and would at least require some form of consent.

From PII to uniquely identifying an individual (the legal bit)

Rules and regulations of advertising health related products differs in the US and in Europe; even the basis of when and where data privacy legislation comes into effect follows totally different ideologies.

The US focuses on limiting the liability of companies using data, through a variety of sector based Privacy legislation of which HIPAA – The federal Health Insurance Portability and Accountability Act of 1996 – is the most well-known. US Privacy legislation is called upon once some form of PHI - Protected Health Information - is collected. When the individual is identifiable Personally Identifiable Information (PII) legal experts are consulted. In the absence of PII, there is no concern over privacy legislation in the US.

The EU focuses on protecting citizens through overarching directives and regulations – typically the Data Protection Directive (DPD - enacted in 1995) and the currently proposed General Data Protection Regulation (GDPR). Europe takes a broader approach to PII: it depends "upon whether a natural person is capable, directly or indirectly, of identification through a linkage or some other reference to available data". PII logic is based on ill-defined variables and a concept that does not hold under European legislation, including in the UK.

Understanding your companies' role within the data ecosystem

While risks of identifying individuals increase as more data is collected and centralized, as the recent UK based NHS scheme called care.data revealed, the first step is understanding your companies' liability for the data that is being collected, processed and possibly shared between systems, either through national borders or with other legal entities.

Talking about digital, companies often find it difficult to understand what their corporate, pathology or disease related properties are collecting in terms of data.

The way in which websites and mobile apps are built have consequences on what type of data is transiting between visitors of a particular app or property and the company responsible for the available online information.

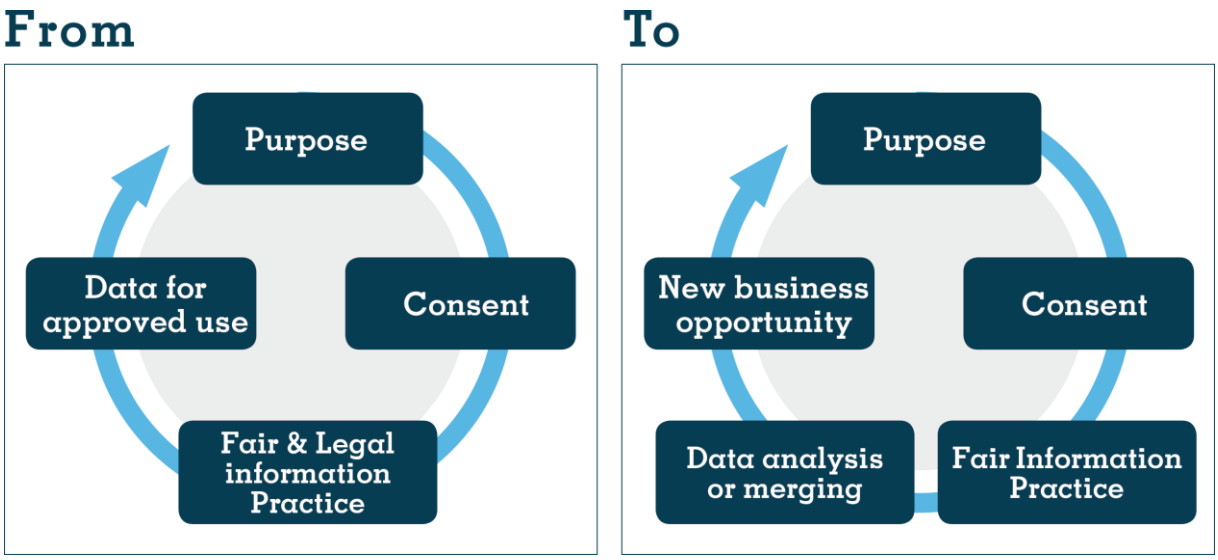
Following European privacy thought process, the company putting available information accessible to online users is considered to be a "**Data Controller**".

Independent of evolving legislation, in Europe but also increasingly in Asia and Latin America, the principles that the EU Data Protection Directive requires data controllers to observe, when processing personal data, reflect good business practices.

They contribute to reliable and efficient data processing, which is useful in our increasingly data-driven world. It also has the benefit of protecting the rights of those about whom the data is collected, the **data subjects**, fostering trust and avoiding brand erosion through unsystematic privacy management practices.

Loosely described and dependent upon how the current Data Protection Directive has been transposed into local law, digital marketers, as **data controllers**, must keep in mind some basic principles related to:

- **Understanding how close the data uniquely identifies an individual**. Hence, as more data is shared and merged, this becomes a probabilistic exercise instead of an on/off type of task like PII;
- **Defining purpose and consent for collected data:** know what you're going to do with the data today and revisit the purpose for future uses;



Is big data killing the privacy framework of purpose and consent?

- **Understanding data types and categories:** how should information security measures and consent be adapted according to data types? Are we talking about explicit or implicit consent, opt-in or opt-out? Should the data be secured while in transit? Should it be anonymized if shared with another company, even only for processing purposes?

- **Improving data quality** by updating the data when necessary and allowing data subjects to rectify or remove data about themselves;

- **Reducing risk of data breaches** by not keeping the data any longer than necessary (respect data retention periods);

- **Protecting the data through adequate information security measures** where protective measures should be aligned with data types;

- **Responding to complaints or requests from data subjects** this is probably going to increase as more consumers are asking questions about data uses. Is your company ready?

- **Notifying national authorities when processing personal data** this can be paid for or free, depending upon the country;

- **Notification in case of data breaches**, as US health insurer Anthem recently did after their 80 million records hack: http://anthemfacts.com/. Make sure your company has a crisis plan in case of a data breach.

In addition, companies and the **data controllers**, use intermediaries such as digital agencies but also tools in order to support their digital communications.

Starting with any information that might be collected, digital marketers need to make sure these data collection practices are in line with what is stipulated within their policies. After all, they are liable for anything that might be out there, collected, processed or re-used on their behalf.

Such intermediaries, also called **data processors**, are separate legal entities from the **data controller** and process personal data on their behalf.

Additionally, the **data processor** become partially responsible for the safeguard of the data collected, depending upon the legal contracts set-up between the various intermediaries (sometimes 3rd, 4th and 5th parties) and the initial **data controller**.

If for example the data collected is stored within the cloud and could possibly fall under another legal jurisdiction as the one where the initial data collection took place, it is the duty of the **data controller** to assure the same rights are assured, even under this extra-territorial storage facility.

It is therefore crucial to understand exactly what data is collected, even if not processed, where this data resides and who has access to it. Such undertakings are usually referred to as defining the data flows.

From 100% compliance to risk based data uses

While Europe is trying very hard to become the international reference for a Data Protection framework, there is one set of rules called Fair Information Practice Principles (FIPs or FIPPs) that are globally agreed upon.

Indeed, even the revised OECD Privacy Guidelines issued in 2013 references to the Fair Information Practices, which contain the following 5 essential points:

1. **Transparency;**
2. **Choice, opt-out vs. opt-in;**
3. **Information review and correction;**
4. **Information Protection;**
5. **Accountability**

For global companies managing data on multiple continents and in a variety of countries, reality shows that 100% compliance with each local and evolving data privacy legislation remains unrealistic.

While respecting FIPPs should be considered as an initial best practice, a lot of data-driven companies are today focused on risk management exercises related to privacy.

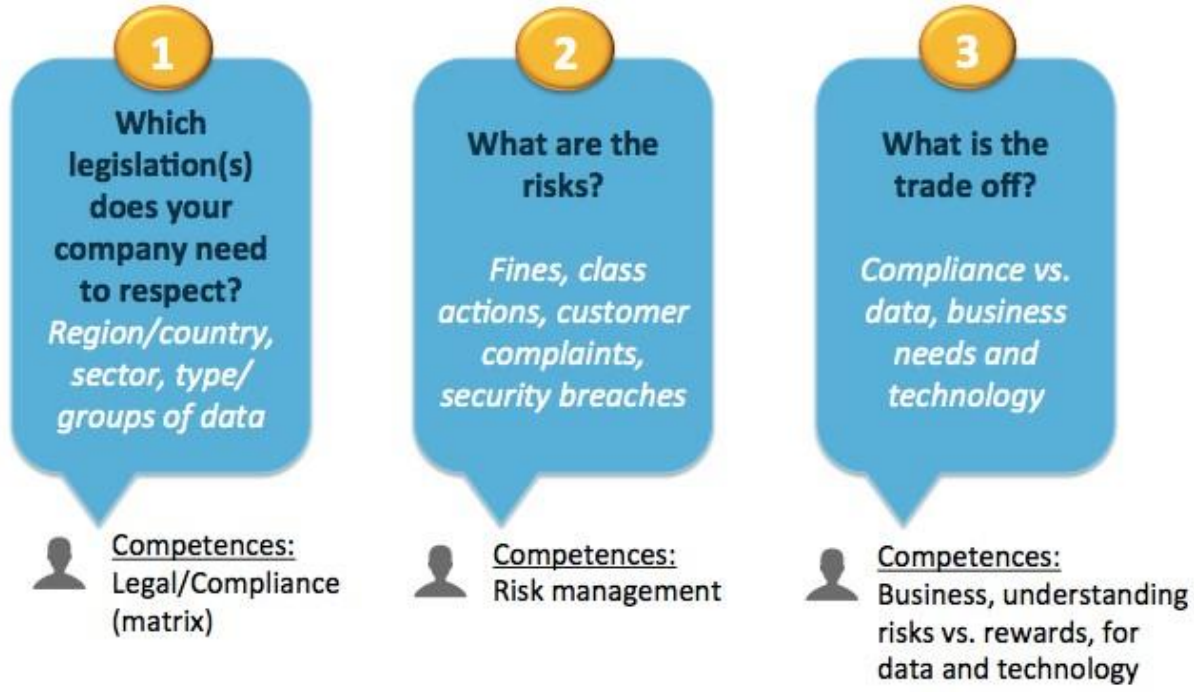
As systems are rolled out globally (or per continent), it is nonsensical to set too many exceptions for smaller countries where the risk of perceiving any kind of privacy backlash is unlikely to exceed amount to more than 500 euros. Typically, companies do not set-up exceptions for countries such as Slovakia, except if they have a good reason to do so.

The way to look at privacy in our digital age and to move the subject further is therefore to understand the data flows, which data type where and accessed by whom, and embed this tactical understanding into a larger **3 step risk management framework**:

1. **Which legislation(s) applies to your company?** Typically grouped per region, country, sector and type/groups of data;

2. **What are the risks of non-compliance?** Understanding the fines, class actions, customer feelings of creepiness or security breaches that might occur?

3. **What is the trade off?** Typically trade-offs and decisions depend on sector and a companies' appetite for risk.



Want help with these or other data issues?

Get in touch with one of our experts for a no-obligation chat about how we can help you with your data privacy needs.

About our guest contributor

*Aurélie Pols, from Mind Your Privacy, has an econometrics and statistical background on top of a Master in eBusiness from the Solvay Business School in Brussels. Having specialized in digital analytics for over a decade, she focuses today on the Privacy aspect of Big Data by bringing her international expertise to support client projects within both Mind Your Privacy and Mind Your Group, one of Blue Latitude's specialist **partners**.*

*Follow **@AureliePols** on Twitter*