DIGITAL ANALYTICS ASSOCIATION

SIGEU Whitepaper on privacy compliance

In the EU people are concerned about their online privacy. The EU has set new laws on Privacy. It is important for businesses and organizations to understand how to be compliant with these EU laws and regulations.

Authored by: Geddy van Elburg

401 Edgewater Place, Suite 600 ▪ Wakefield, MA 01880
Phone: +1 (781) 876-8933 ▪ +1 (800) 349-1070 ▪ Fax: (781) 224-1239
www.DigitalAnalyticsAssociation.org

License

I thank Jim Sterne, Stina Ehrling, Anna Long and Matthias Bettag and all the EU SIG members for contributing, their help and support.

Contents

Introduction

Purpose

As with most discussions of privacy in the online context, an accurate understanding of the issues require both technical and policy knowledge. The goal of our efforts is not to recommend tools, but provide a deeper understanding of the privacy laws as they are made in the European Union. As this matter changes constantly, this is a work in progress. We recommend updating your knowledge per country where required.

Whether you're a marketer, analyst, programmer, business analyst or dealing with personal information in any way, it's crucial that you understand the impact of your decisions on the privacy of your users and clients. The privacy issue should be on the agenda of every company or organization. As a (web/digital) analyst, it is important to know how to be compliant with multiple privacy laws in different countries. But privacy is more than a cookie on a website. It also involves managing data analyzing, storing and processing.

DAA and the EU SIG

This document, though it comes from the DAA European Special Interest Group (EU SIG), does not prescribe standards for privacy policies or privacy practices of analytics tools and services. As a digital analyst is considered a steward of personal data of visitors, knowing about privacy implications is an important a part of the job description.

Intended audience

This whitepaper is for digital analysts, as well as those outside the profession, to gain a better understanding of the consequences of the issues.

Privacy should be on the agenda of every company or organization that stores data about individuals or uses tracking methods on websites, mobile apps etc. As a digital analyst, it is important to know how to be compliant with multiple privacy laws in different countries. But privacy is more than a cookie on a website. It also involves analyzing, storing and processing data.

This whitepaper intends to help European and non-European analysts better understand the matter and the privacy landscape in Europe.

Privacy is a major concern by politicians in the EU, but even more so by the public. Being compliant is not only a legal issue, it is an essential way to respect your visitors, customer and clients.

Privacy is more than a cookie on a website

The privacy debate has been focusing on the cookie issue, but this is only one part of the complete privacy topic. The main issue is the collection and processing of personal data. The main issues come from these questions:

- What data is collected?
- What is the data used for?
- Where is the data stored?
- How long is the data stored?

When your organization or business is collecting data from their users or clients, you have to conduct an audit and make sure this data is collected according to national laws and stored and handled accordingly.

Privacy as a fundamental right

In Europe, protection of personal data is a fundamental right. This reaches beyond the "right to privacy". In the Charter of Fundamental Rights of the European Union Article 8 clearly states the privacy rights of the individual.

The fact that data protection is a part of the Charter of Fundamental Rights indicates the importance of the issue.

What is personal data?

Any information relating to an individual, whether it relates to his or her private, professional or public life, is considered personal data. As an example: name, address, email address, bank details, posts on a social network website, medical information, religious information and IP address of a computer all are considered to be personal data.

Article: Protection of personal data

Everyone has the right to the protection of personal data concerning him or her.

- Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.
- Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- Compliance with these rules shall be subject to control by an independent authority.

In the EU all data which makes it directly or indirectly possible to identify a person is subject to the privacy laws and the fundamental right of privacy.

Europeans and Privacy

History

Privacy in the EU is described in article 8 of the European Charter and is a fundamental right, just like the freedom of speech, etc. Therefore, special legislation is in place to ensure the privacy of individual people is protected. In the US, privacy is not a specific governmental regulation but rather a combination of legislation, regulation, and self-regulation. The stricter views on privacy in the EU originate in history.

Europeans encountered the dangers associated with uncontrolled use of personal information stored in (paper) databases. During World War II, fascist's governments used this information on race, ethnicity and religion and many people saw family, friends and neighbors transported to concentration camps. When computers came along, the distrust of the abuse on Personal Information by corporate databases and governments led to new regulations on protecting personal data.

This is the fundamental issue that Americans do not immediately grasp. The EU laws do exist because of a lack of trust in corporations and governments who have misused this information in the past.

Since the early years of the Internet, the EU started to regulate privacy in this specific area. Since the directive 95/46/EC on personal data protection was adopted in 1995, the EU has continued working on a comprehensive data protection scheme. As the influence and the Internet itself evolved, new directives were announced and put in place. The latest is Directive 2009/136/EC of November 2009, based on previous directives 2002/22/EC and 2002/58/EC. This latest directive was incorporated in the national laws of the member states in May 2012.

An EU directive always needs to be translated into the national laws per country. An EU regulation is an EU law which will be compliant in all the EU countries alike.

Intention of the Privacy laws

The intention of the new EU directive and EU country laws on privacy is to protect the public against the abuse of private information. Benign anonymous aggregate reports from an analytics tool are not regarded as the target of the Directive. But in some of the EU countries the laws are stricter on this. They see even *anonymous* tracking as an issue requiring explicit consumer consent.

The Public

Even though a majority of European Internet users feel personally responsible for the safe handling of their personal data, almost all Europeans are in favor of equal protection rights across the EU (90%). When asked what type of regulation should be introduced to prevent companies from using people's personal data without their knowledge, most Europeans think such companies should be fined (51%), banned from using such data in the future (40%), or compelled to compensate the victims (39%).

- 26% of user of social media feel in control towards their data protection.
- 18% of the online shoppers feel in control.
- 74% of all Europeans see personal data disclosure as an increasing part of modern life.
- 72% of the European citizens feel they give away too much personal data
- 33% are aware of the existence of a national data protection authority in their country
- 90% want the same data protection rules across the EU

Source: Special Eurobarometer 359: Attitudes on data protection and Electronic identity in the European Union, June 2011

Example

A web shop in country X with shops in 14 EU countries collects data of clients in these 14 countries.

Although this data may be transferred to and processed in HQ in country X, this company has to be compliant with processing of data in all 14 countries.

Businesses and organizations should be aware of **this major concern about their personal data** when they use personal identifiable information for commerce. Companies and organizations that handle personal data with care and are transparent about what is done with this data, how it is stored etc., treat their users/visitors with respect.

People want to know why, when, and which personal data is used and where and what it is used for. In the Special Eurobarometer Survey, 70% of Europeans stated they are concerned that their personal data held by companies may be used for other purposes than that for which it was originally collected. They feel that their data is better protected within governmental organizations and larger businesses. As more than 90% of all companies in the EU are Small or Medium Enterprises (SME's), this shows a great breech in trust.

The "Cookie Laws" of 2012

As the directive had to be translated into national regulations, the expected result was a patchwork of different laws. For international oriented businesses this means a great constraint on their organizations. These different laws are quite a burden on businesses outside the EU as it is difficult to figure out when and how to be compliant.

These laws (May 2012) were commonly named “cookie laws”, as the public debate became popular. The problem with this misnaming is that many companies only focus on compliance with cookies, and do not think of the privacy issue as a whole or of the impacts this might have on their analysis or marketing efforts.

When do you need to be compliant and to which law?

Most of the businesses think they have to be compliant only with the laws governing the geographical location of their headquarters. This is not true. **When you are targeting a specific country, you have to be compliant with the laws of the targeted countries.**

This might be quite a challenge as the 27 different countries in the EU made different laws based on the same EU directive.

Cookie law: DNT (Do Not Track);Opt-in or Opt-out?

As the public debate is mainly about the “cookie laws”, we will tackle this issue first.. Based on the different countries interpreting the directive into different laws, we separate them into six groups:

1. Not Clear/ Unknown

   The implementation of the law is not finished or is not clear/ unknown at this moment. (Belgium, Bulgaria, Cyprus, Germany, Iceland) This means the directive itself will be the guideline to compliance.

2. Opt-Out by Browser

   Cookies may be set, but you have to inform the visitor clearly about your use of cookies and inform them how the user may decline cookies in their browser. This applies to first party and third party cookies. (Czech Republic, Denmark, Estonia, Finland, Hungary, Ireland, Italy, Liechtenstein, Luxembourg)

3. Restricted Opt-Out by Browser

   Anonymous first party Cookies may be set, but you have to inform the visitor clearly about your use of cookies and inform them how they may decline cookies in their browser. Explicit opt-in is required for Third party cookies and non-anonymous cookies. (Poland)

4. Opt-Out on Website

   Opt-out must be provided on a website for first and third party cookies. Browser setting is not sufficient: (Latvia, Malta (?), Spain, Sweden, although Swedish government uses opt-in to be on the safe side.)

5. Strict Opt-In

   Browser setting is not sufficient, but there are exceptions based on functionality. (France, UK, Greece, Lithuania,

6. Strict Opt-In Except for Functional Cookies

   Strict opt-in for all cookies, except functional use on website e.g. ecommerce, browser setting is not enough and website owner has to prove the given consent. (Netherlands) In all cases providing clear and understandable information is required and absolutely necessary. Note: Norway is not an official EU country. Their privacy laws are strict. Opt-in is needed (category 5)

Although these laws are called “cookie laws”, data collection is not solely restricted with the use of cookies. Whether data is gathered by the use of cookies, pixels, finger printing, flash cookies or any other technology, compliance with the privacy law is obligatory.

How to deal with compliance

How do you, as a business, comply with privacy laws as far as cookies (and other tracking methods) are concerned? The location of HQ or the location where the data is stored or processed is not an issue in compliance. Where you gather your data and where your targeted audience live are more important. If you are tracking EU citizens, even if you are a non EU company, you'll need to be compliant with EU laws.

Defining your targeted countries

Your first step is to list your targeted countries. Is your website translated into multiple languages? Do you advertise in multiple countries? Do you have offices or shops or physical post addresses in those countries?

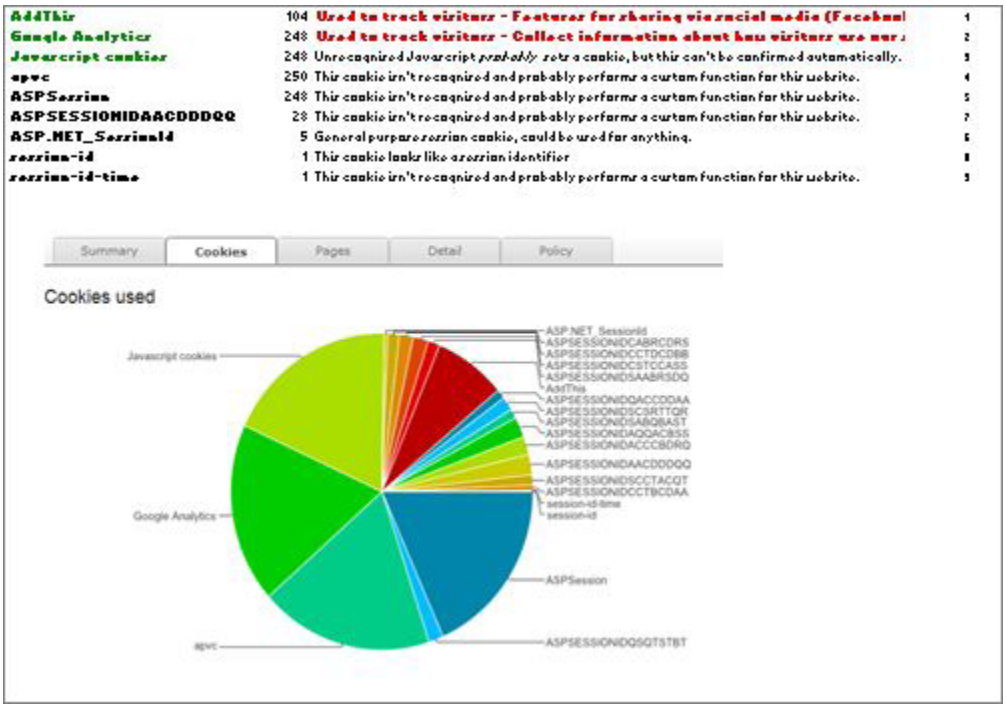
Look up the cookie laws in those countries. (Do make use of an Internet lawyer!) You might have to implement multiple ways to be compliant.

As a business you do not want to overdo the privacy settings in a competitive surrounding when it is not required by law. For instance when you are targeting Finland, where no explicit opt-in is necessary and your competitors won't have opt-ins on their website, you probably will not want one yourself.

Make sure you can differentiate your opt-ins and opt-outs according to the targeted countries. This will effect on the technical aspects of your website.

Cookie Audit

All countries require clear and understandable information on which cookies you use and how the user can preclude cookies. You have to provide a solid privacy statement in which you explain which cookies you are using and what they collect. More important, if you collect personal data (your email form/ shipping address etc.) you must clearly state who has access to these data and how you are going to use it.



First party cookies

Most websites set first party cookies. This might be a session cookie or a shopping cart, etc. Without these cookies the site will not function properly.

Most users need to use them in order to browse and use websites. You won't need consent to use these cookies.

But using first party tracking cookies such as Google Analytics might need consent depending on the targeted country.

Third party cookies

Social plugin buttons such as tweet me, follow me, like, Google plus and LinkedIn often set 3rd-party cookies. Adwords retargeting and other optimizer tools will set third party cookies. If you embed any of the above 3rd-party networks/plugins into your site, explicit consent must be given by the website visitor.

This is because they are not first-party techniques and so there might be privacy implications for visitors having their behavior profiled on different unrelated websites across the web. This always requires explicit consent.

First party cookie:

Also known as HTTP cookie, web cookie or browser cookie, the First Party Cookie is usually a small piece of data sent from the website you are visiting. These might be functional cookies essential to the website or tracking cookies for anonymous tracking of visitors within the same website.

Third party cookie:

Third-party cookies are set from different domains from the one shown on the address bar (i.e. content from a third-party domain e.g. an advertisement run by www.adexample.com showing advert banners. If you are using third party cookies, even if it is only collecting anonymous data, you'll always need explicit consent. E.g. opt-in.

At this moment it is not clear who is responsible for these third party cookies. But as you have placed the icons on your website or embedded the video, you may be held accountable for them. Be aware: *If you are using third party cookies, you'll always need explicit consent even if you are only collecting anonymous data.*

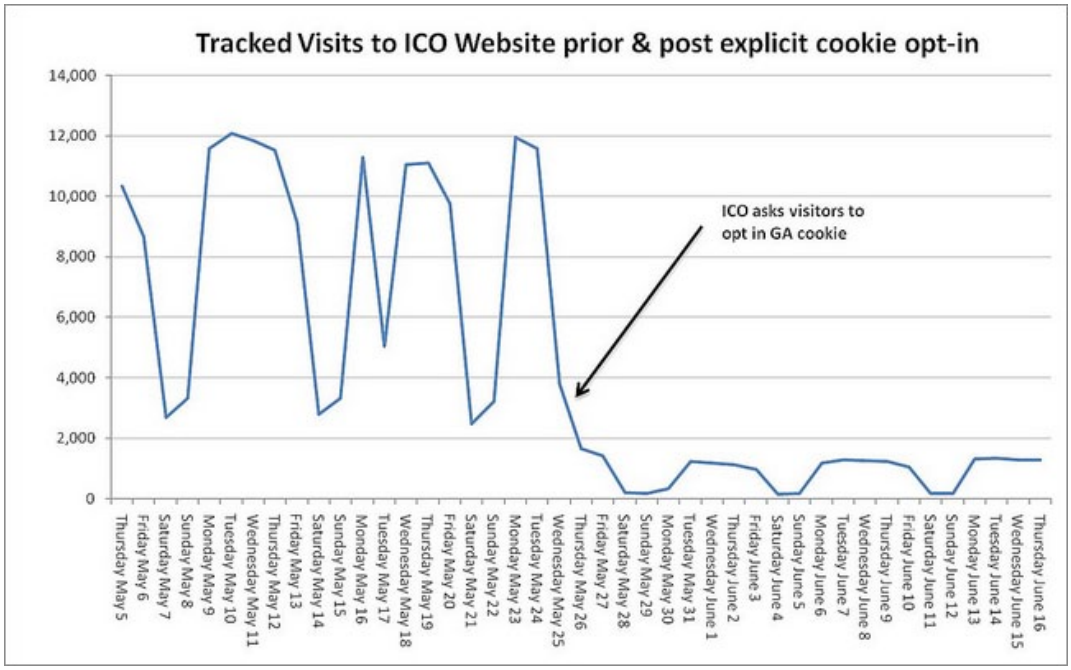
Analytics

Many website owners make use of an Analytics tool. As long as the collected data is anonymous and sets first partly cookies, you'll be fine in most of the EU countries. This was the intention of the directive. However a few countries like the UK and the Netherlands see anonymous tracking as obtrusive and require explicit consent. If cookies are not *completely* anonymous or are not first party (set by your own website domain), you **always** need explicit consent from each visitor in all the countries in the EU. The way they give their consent may be done in different ways (opt-in/opt-out/DNT in browser setting)

Effect of the directive 2009 on "cookies"

The implementations of the directive in the different countries have effects on businesses. The EU SIG is seeking information about the effect on individual businesses; not only on measurement of their traffic, but also on the effect on their conversions, etc.

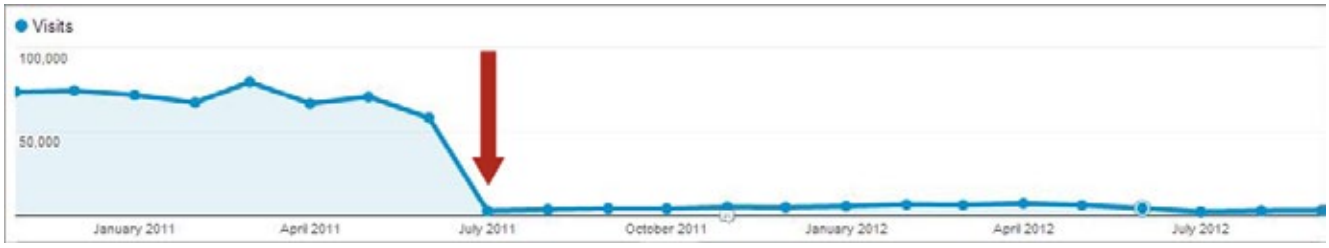
The first sign of an explicit opt-in before any cookie may be set, is dramatic. The Information Commissioner's Office (ICO) in the UK lost 90% of their data.



** Thanks to Vicky Brock who acquired this data from the ICO*

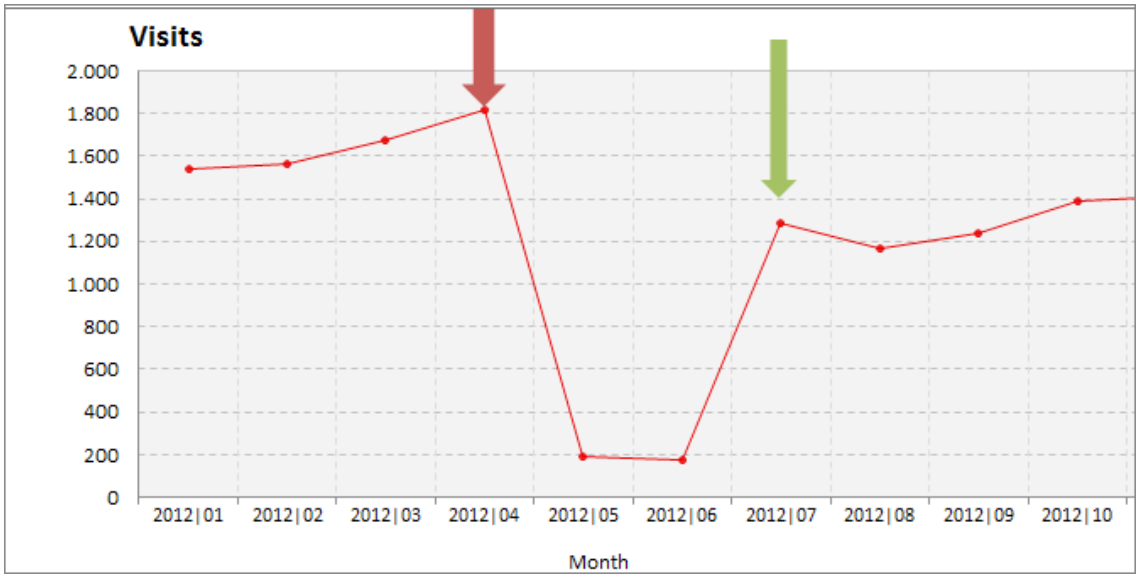
Governmental organization

The same results were seen in Sweden for the website of the government.



The Swedish government lost 90% of their data on website users. This makes it impossible to know if millions of tax payers' money is well spent on the websites. The numbers are still large enough to do some trend analysis, but A/B split testing or multivariate testing has become nearly impossible.

Commercial website of B2B business (SMB)



In this example we see a sharp drop of visitors after implementing an opt-in on first party cookies used for trend analysis. (Red arrow) After the opt-in was changed into an opt-out we saw a partial restoration of data. (Green arrow)

Advertisement Industry

In addition, accountability of online advertising might drop by 85%. Getting consent is not easy.

Test results in the Netherlands on a large information website showed the public was not interested in accepting or denying cookies. Most of the visitors to this website did nothing. They just browsed the website, without giving consent or denying cookies.

The public is not sufficiently aware of the use of cookies and feels threatened. Incorrect information through the media misinforms the public. Because of the misunderstanding of different kinds of cookies, visitors decline consent when interrupted, and fail to complete their desired task. Asking to accept or decline cookies is interrupting the task the visitor is trying to perform. Instead of accepting this interruption, he or she continues their way, without giving consent.

More testing needed

We need more test results on the effect of the data protection laws as they are now. In the next two years, the EU Data protection directive2009 will be replaced with the EU Data protection regulation. Businesses and organizations have plenty of time to prepare and to test the best way to provide data protection to the public.

Data protection: Not only about cookies

Note that Article 8 prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life unless one of the exception criteria is met.

Article 7:

Collecting and Processing the Personal Data of Individuals

- Where the individual concerned, (the 'data subject'), has unambiguously given his or her consent, after being adequately informed; or
- if data processing is needed for a contract, for example, for billing, a job application or a loan request; or
- if processing is required by a legal obligation; or
- if processing is necessary in order to protect the vital interest of the data subject, for example, processing of medical data of a victim of a car accident; or
- if processing is necessary to perform tasks of public interests or tasks carried out by government, tax authorities, the police or other public bodies; or
- if the data controller or a third party has a legitimate interest in doing so, so long as this interest does affect the interests of the data subject, or infringe on his or her fundamental rights, in particular the right to privacy. This provision establishes the need to strike a reasonable balance between the data controllers' business interests and the privacy of data

Future on Privacy law in EU

Because it is very difficult to be compliant with different national laws and because the public really wants protection of their data wherever it is collected or stored or processed, the EU commission made a proposal for a new EU regulation on privacy. There are two starting points:

1. Effective protection of the fundamental right of individuals to protect their data
2. Economic market. The growth of the digital economy asks for a single regulation of privacy as data might cross borders.

The EU commissioner understands the threat of multiple laws to the EU internal market. It also lays a heavy burden on businesses to comply with multiple laws. It is confusing for businesses outside the EU to know how and where to be compliant.

The new regulation (EU law) is going through all the political EU channels and is expected to be effective in 2014.

The new Regulation intends to improve the quality of information to the public about the data that is provided. The proposal makes sure that personal information is protected, no matter where it is stored or processed (within or outside the EU). The EU commission hopes this will help build trust in the online environment.

Main topics of the new upcoming regulation:

Right to be forgotten: A "right to be forgotten" will help people take control of their data. When people no longer want their data to be processed and when there are no legitimate reasons to retain it, data will be deleted. This will not be the case involving journalistic articles or the freedom of speech.

Easy access to one's own data: Everybody has the right to have access to the data that is collected and stored. This must be free of charge. Every business or organization should provide easy access to collected data.

Right to edit one's own data: People have the right to edit the data collected about them. Assuming there is no legal impediment, the individual person has the right to edit or erase his or her data.

Right to data portability: If individuals no longer want their data processed, they can have it transferred to another company/provider/ social medium.

As the new regulation is not yet in force and still might get adapted on the way to the EU Parliament, it is important for organizations and businesses to keep themselves informed.

Privacy by design / privacy as a default

The main point of the data protection laws, or the upcoming new EU regulation on data protection; is that they have the same fundamental, personal data protection as a default. This will mean that all companies should make sure they adjust to this new way of treating data.

Privacy as an Unique Selling point

Handling and analyzing data is always a matter of trust. When your visitors and clients trust you, they might be more willing to provide information you need to analyze your performance, to provide better services, to enhance your customer care, etc

Why being compliant is a way of respect

"70% of EU citizens are worried about the misuse of their personal data. That's why the EU is developing rules to strengthen your right to access, change or delete your data. And it's adding a 'Right to be Forgotten' online…"

With the new upcoming regulation, businesses will have plenty of time to adjust and test the best way to become compliant.

Sources

Websites

EU Fundamental rights

- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

EU data protection law

- http://ec.europa.eu/justice/data-protection/law/index_en.htm
- http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm

Eurobarometer factsheets per country

- http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm#359

Special Euobarometer 359

- http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Studies on data protection

- http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm
- http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

EU factsheets on upcoming data protection regulation

- http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf
- http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf
- http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf
- http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf
- http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf
- http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf
- http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf

401 Edgewater Place, Suite 600 ▪ Wakefield, MA 01880
Phone: +1 (781) 876-8933 ▪ +1 (800) 349-1070 ▪ Fax: (781) 224-1239
www.DigitalAnalyticsAssociation.org