EU Data Protection Regulation - do we or don’t we have privacy? An update

ISACA Winchester – 19th February 2014

Sarb Sembhi, Director of Consultancy Services
Incoming Thought

©Incoming Thought Limited 2014. www.incomingthought.com
Usual Disclaimer

• All thoughts and comments are my own personal thoughts and comments
• No part of this presentation is intended to be provide legal advice, please check all information with a legal professional before considering acting on any information provided
• This is a general presentation and must not be considered as professional advice for and specific aspect of your business
Introduction

• Is privacy dead?
• Security vs Privacy?
• Privacy Day anyone know?
• Anyone fed up of trying to keep up to date with this topic?
• Anyone confused with what is going to happen with the Regulation?
• Don’t despair, we are all in the same boat, so let’s have some fun instead
Outsourcing Firm Ventas Central Update Policies in Preparation for Changes to EU Data Protection Rules

Ventas Central is prepared for the changes to the EU Data Protection Rules. The firm rolled-out updates to their data policy last week to keep up to date with future regulations that will be enforced to all business within the European Union.

9 JUL 2013 WDM Group PR Network

ESSEX, ENGLAND, July 04, 2013 /PRNewswire/ -- In January of this year, the European Commission revealed a draft of its European Data Protection Regulation to replace the previous Data Protection Directive. The European General Data Protection Regulation represents the most significant change to data protection in the UK and EU since 1995. Once adopted, it will have the force of law across all 27 EU Member States, giving uniformity of data protection laws across all Member States and significantly increasing penalties for non-compliance. The legislation process is likely to take up to two years to complete with another two years being spent bringing the new regulations into effect. Therefore it is unlikely that it will be in force before 2015.

The aim of the new European Data Protection Regulation is to harmonise the current data protection laws. At Ventas Central, few changes will need to be made to comply with the new regulations since their data
Steelie Neelie: One cloud contract model to rule them all

The road to hell's paved with good intentions, though

By Paul Kunert, 24th June 2013

The European Commission is seeking leading lights in the arena of cloud services to help sketch out a contract framework so that customers don't get tied into murky deals.

At least, this is the principle that Steelie Neelie Kroes, vice president of the EC outlined in a blog today, ahead of the European Cloud Partnership Steering board in Estonia next month.

"One of the big barriers to using cloud computing is a lack of trust," she said. "People don't always understand what they're paying for, and what they can expect."

"I think you should be able to know what you're getting and what it means - and it should be easy to ensure that the terms in your contract are reasonable: open, transparent, safe and fair."

A "formal expert group" is to be set up to undertake this task, which the EC said is particularly sought after by SMEs.

These small biz owners may "hesitate to use the cloud because of fears that they will not meet legal obligations, or who might be worried that they get locked in or stranded by changes of technology or service by cloud providers", said Kroes.

She said SMEs don't want to take the risk of "getting mired in foreign court cases", are fearful of exposing their data to security risks or breaches and can't afford to
Merkel says Europe’s trust must be repaired after U.S. spying claims

Posted on: 3:17 pm, October 24, 2013, by Staff Writer

(CNN) — German Chancellor Angela Merkel said Thursday that trust between Europe and the United States must be "reestablished" after claims the U.S. National Security Agency eavesdropped on her cellphone.

Merkel commented as she arrived at a summit of European Union leaders in Brussels, Belgium, which risks being overshadowed by anger about allegations the United States has been spying on its allies.

“We need trust, and now the trust has to be reestablished,” she said. “Spying among friends is never acceptable.”
EU to push ahead on data protection despite UK opposition

Published 28 October 2013, updated 06 November 2013
Tags Data protection, European summit

SPECIAL REPORT / The European Commission is set to ignore attempts to delay the implementation of a proposed new data protection regulation (DPR) suggested at last week’s EU summit, claiming that the meeting’s conclusions have been misinterpreted.

EurActiv has learned that the EU executive instead believes that a mandate to push forward with new rules by spring next year remains possible, and that this can be achieved even in the face of strong opposition from the UK.

Last week saw a tussle over the wording of the European Council conclusions – before the summit started – with the Commission calling for the DPR to be completed by “spring 2014”.

>> Read: Data protection: France, UK lead rival camps at summit

The move is seen as critical since delaying the agreement of new rules until later next year risks passing the dossier to new commissioners who will take up their posts at the beginning of 2015.

Conclusions suggested delay until 2015

Many analysts believe that the proposed DPR would need to be re-drafted from scratch by a new Commission, leaving the current proposal effectively wasted.

The final conclusions adopted last week suggested that the DPR should be introduced “by 2015”. Indeed France’s president, François Hollande, told a post-summit briefing that the new wording meant that the new rules should be in place by the beginning of that year.

The French president put a positive gloss on the delay, claiming that some countries had been calling for the DPR to be introduced “as soon as possible”. Since such a formulation was meaningless, he said, it was far better to have a firm date than none.

EU sources have told EurActiv, however, that the wording of the conclusions leaves open the opportunity to introduce the DPR earlier than 2015.

Leaders agreed: “The timely adoption of a strong EU General Data Protection Regulation is a priority for all member states and will be supported by the European Commission.”
EU tsars rubbish Brit PM over attempt to delay beefed-up privacy rules

Privacy? Data protection? Sod 'em - there's an election coming, donchакnow

By Kelly Fivush, 26th October 2013

Internet security threat report 2013

Sources close to EU justice commissioner Viviane Reding have dismissed reports suggesting her proposed overhaul to the bloc’s data protection laws has been stalled, after Britain’s Prime Minister appeared to have postponed the regulation.

Late on Friday, the Financial Times reported that David Cameron had apparently convinced the European Council to block any swift adoption of the draft data protection rules.

But The Register has been told in confidence that such a claim “has nothing to do with reality.”

We've asked Number 10 to clarify the PinkUn's story, which cited an unnamed US tech exec who said that “Britain's common sense prevailed” at the summit – which itself was overshadowed by allegations that Germany’s Chancellor Angela Merkel had her phone tapped by US spooks.

At time of writing, Downing Street had not responded to The Register's request for comment.

Last week, MEPs voted in favour of ripping up existing data protection laws in Europe that were introduced in 1995, after the parliament’s civil liberties committee made nearly 4,000 amendments to Reding’s draft bill.

The lawmakers have been lobbying in recent months for tougher controls on privacy-
Google privacy chief: Proposed EU privacy law 'dead'

Peter Fleischer, Google's top global privacy counsel, says a "much-flawed" proposed EU privacy law is "dead," while praising whistleblower Edward Snowden.

©Incoming Thought Limited 2014. www.incomingthought.com
EU admits Google fines are 'pocket money', urges data protection reforms

by Dan Worth  20 Jan 2014

Europe needs a much harsher regime to fine businesses that breach data protection laws, as recent penalties handed out to Google are nothing more than "pocket money" to the company.

EU justice commissioner Viviane Reding said plans to reform the data protection laws in Europe must be pushed through, otherwise firms will continue to ride roughshod over the laws as they exist.
British Judge Rules Google Can Be Sued In UK Over Privacy Case
from the setting-precendents dept

The battle over online privacy, and how personal data should be treated as it moves over the Internet, is being fought between the US and EU points of view in multiple ways. There is the EU's Data Protection Regulation, currently grinding its way through the legislative process; there are the discussions about the NSA's spying program, and how it impacts Europeans; and finally, there are various court cases involving US companies and the personal data of EU citizens. One of these is in the UK, where The Telegraph reports that an important decision has been handed down:

The High Court ruled on Thursday that Google can be sued by a group of Britons over an alleged breach of privacy, despite the company being based in the US and claiming that the case was not serious enough to fall under British jurisdiction.

Google faced a group action by users of Apple's Safari browser who were angered by the way their online habits were apparently tracked against their wishes in order to provide targeted advertising. But because Google is based in the US they needed to seek the court's permission to bring the case in the UK, something which the search company claimed was inappropriate.

That claim has now been thrown out, as Mr Justice Tugendhat, sitting at London's High Court, ruled that the UK courts were the "appropriate jurisdiction" to try the claims.

Google has said it will appeal, so it's too early to tell what the impact of the UK courts' decision will be. But if it is allowed to stand, it will create a hugely important precedent for future legal actions against US companies providing services involving the handling of personal data in the EU.

Follow me @glynmoody on Twitter or identi.ca, and +glynmoody on Google+
So, what’s out there 1

• Telephone Call time, date, duration, originating / destination number, possibly content of call (VOIP, wiretapping)
• Unencrypted emails (Gmail, Hotmail, Yahoo, etc.)
• Perhaps even encrypted emails
• Calendar and contact data
• Other unencrypted traffic
• Including: access to all social media sites, uploading utilities, etc.
• Data collected by mobile device applications
So, what’s out there 2

- Data collected by mobile operating systems
- Data stored by backup sites
- Data collected by voip services
- Data collected by mobile payment services
- Search request data
- VPN log data
- This is regardless of business cloud services
Let’s look at Google 1

- Google’s megalomaniacal “mission is to organize the world’s information and make it accessible and useful.”
- Consider the depth and breadth of intimate information Google collects:
  
  **What you search for;**
  
  (a Ponemon Institute survey of 1,000 Google users found that 89% thought that their searches were private and 77% thought Google searches could not reveal their personal identities – wrong on both accounts.)

  **Everywhere you go on the web;**
  
  Google has pervasive unauthorized-web-surveillance capability (web tracking/stalking) through a combination of Google’s search, Google’s cookies, DoubleClick’s ad-view recording capability, Google’s extensive content affiliate network of hundreds of thousands of sites, and the wide variety of Google apps.

**What you watch** - through YouTube;

(Remember Supreme Court nominee Robert Bork was politically attacked for the videos he rented.)

**What you read** - through Google News, Feedburner and Blogger.

**What you say** - in your emails through gmail’s automated reader.

**What you produce** - in Google Docs or spreadsheets.

(In return for the free Google Apps like Docs and spreadsheets, users grant Google some search rights in perpetuity to any content a user produces using Google’s Apps.)
Let’s look at Google 2

What your family and friends look like - through Picassa images.
Your medical conditions, medications, and medical history - through Google Health.
Your purchase habits - through Google Checkout.
Your call habits and voiceprint - through Google Talk.
Your travel habits and interests - via Google Maps.
Your interest in other people/places - via Google Earth & StreetView.
Your personal information - through Orkut (social networking) Gmail, Google Checkout, etc.
Where you go/hang out - through Google wireless ventures and Android.
Where you’ll be or where you were - through Google Calendar.

• Source: www.precursorblog.com
What’s coming next?

- Data collected by Google Glass
- Data collected by smart tv’s (which watch you viewing TV)
- Data collected by smart meters & smart grid
- Data collection by driverless cars
- Data collected by Internet of Things devices around the home
- Data collected on wearable health devices
- Mobile Payments (like Oyster card data)
- Advanced Big Data analysis and data mining tools
- Criminal use of above tools to create new business models based on data stolen from above sources
We can trust businesses, they won’t do evil things with the data. They will lose customers if they abuse our trust?
Imagine the following scenario: A powerful Chinese company acquires a 95% stake in the US market for search advertising. At the same time, it signs up millions of users for its free email service, a version of which is also adopted by many American schools.

The company then captures a commanding lead in the US smartphone market with an operating system that is free and ad-supported. Leveraging sophisticated data mining algorithms that monitor its users' online behaviour, the Chinese company quickly builds a US business worth tens of billions of dollars per year, leaving its American competitors far behind. To support this business, the company builds several large data centres in the US and hires thousands of local sales representatives. Thanks to a clever use of loopholes in US tax law, the company pays only a fraction of its US sales in corporate income tax.

Then one day the company announces a sweeping revision of its privacy policy, granting it the right to combine personal data collected from its user base to enable more accurate ad targeting. At this point, a small federal agency concerned with the enforcement of US privacy laws asks whether the Chinese Internet giant might temporarily delay the new privacy policy while the agency reviews its proposed policies. The agency makes clear that it is not challenging the Chinese company's right to pursue its profitable business model. It merely wants to ensure users have been properly informed and have consented to the public use of their data.
It couldn’t happen here 2

• The company waves aside this request, and the agency is forced to initiate an investigation. After careful procedure and review, the federal agency concludes that the firm has violated US privacy laws. It fines the company $150,000 -- roughly what the giant earns every few minutes.

• How does the Chinese Internet giant respond? It instructs its lawyers to inform the federal agency that American laws do not apply to it, because even though its data centres are in the US, legally its services are provided from China by its parent company. The company decides it does not recognize US regulation standards.

• You might think this scenario is implausible, especially in the US, but right now it is currently taking place in Europe. In fact, if we replace "Chinese company" and "US market" with "US company" and "European market," we can see a parallel scenario unfolding in the European Union's current dispute with Google over its privacy policy.

• [Link](http://www.informationweek.com/government/cybersecurity/google---eu-privacy-dispute-may-affect-us-law/d/d-id/1113567)
A backdrop of an uncaring attitude to rights of users about their private data, to a point of absolute disdain of users privacy rights by powerful multinationals.
A backdrop of Data Breaches

• According the Data Loss database, there were 826 data loss incidents in 2010, 1086 data loss incidents in 2011, 1631 data loss incidents in 2012, and 1406 in 2013 (that we know about so far).

• The number of records being breached is regularly in the millions.

• Several data breach reports from last year indicated that either an organisation has already had a data loss (even if they don’t know about it), or will have a data loss incident in the near future.
Unfair advantages

• Businesses outside of the EU do follow EU law thus putting those that have to abide by EU law at a disadvantage

• Those businesses outside of the EU should have to abide by the same rules as EU businesses do when it comes to the private data of EU citizens

• A balance of power over collection and use of private data needs to be restored / maintained

• Also, unfair rights, - US citizens can seek judicial redress in front of an EU court while EU citizens do not enjoy the same privileges in US courts
Changes in economic climate

• Single, double or triple dip recession – we are still in low / no economic growth period still
• Pressures to cut costs
• Pressures to streamline processes
• Pressures to focus on core competencies
• Pressures to explore outsourcing
• All this has led to a greater use of cloud services, many of which are not based in the EU
EU Data Protection Regulation

• Very emotive, depends on your **stake** in the overall scheme of things, and history

• Device manufacturers; Operating system vendors; mobile carriers; app developers; media companies; private investigators; retail companies; profiling companies; banks; health service providers; SME’s; public sector; regulators; citizens; governments; victims; spy organisations; etc. etc.
So where are we now? 1

• Before proposal is formulated, several big business lobby heavily to water down proposals
• January 2012 proposal made public
• April 2013 due to be agreed but delayed due to over 4000 amendments
• May – now, Snowdon revelations
• May – October Regulation tightened rather than further watered down as was likely in April
So where are we now?

- 21 October 2013, the European Parliament’s leading Committee on Civil Liberties, Justice and Home Affairs (LIBE) backs the proposal with an overwhelming majority.
- October 2013, reforms repeatedly discussed and agreed by national Ministers in the Justice Council.
- 24-25 October 2013, European heads of state and government committed to a “timely” adoption of the legislation.
- Under the Presidency of Greece and Italy (six months each) they will work out a roadmap to get an agreement on the legislation.
- The first reading is expected at the April 2014 Plenary session of the European Parliament.
What’s in what’s out?
Some of these things are expanded and clarified for all member states
EU DP Issues Update 1

• New expanded Data Protection Principles:
  – Processed lawfully, fairly, and in a transparent manner;
  – Collected for specified, explicit, and legitimate purposes, and not further processed in ways incompatible with purposes;
  – Adequate, relevant and limited to the minimum necessary;
  – Only processed if, and as long as, the purposes of the processing could not be fulfilled by processing information that does not involve personal data;
  – Accurate, kept up-to-date, with incorrect data being erased or rectified;
  – Kept in a form that permits identification of the data subjects for no longer than necessary;
  – Processed under the responsibility and liability of the data controller, who must ensure and demonstrate for each operation its compliance with the Regulation.
EU DP Issues Update 2

• Requirement for: Specific, Informed and Explicit Consent
• Protection of Children Under 13
• Expanded Definition of Sensitive Data
• Simplification of Cross Border Transfers
• Controllers and Processors to have greater accountability
• Special Rules for Data Processors and Subcontractors
EU DP Issues Update 3

- Obligation to provide adequate security
- Security breach disclosure
- Data Protection Impact Assessment
- Right to lodge a complaint with a Supervisory Authority
- Judicial Remedy against Data Controllers or Processors
- Judicial Remedy against Supervisory Authorities
- Class Actions
- Individuals’ Right to Compensation
- Penalties and Sanctions
EU DP Issues Update 4

• Rights of Data Subjects:
  – Transparency and better Communication
  – Right of Information
  – Right of Access
  – Right of Rectification
  – Right to Object to the Processing
  – Right not to be Subject to Measures based on Profiling
  – Right to be forgotten (not Erasure)
  – Right to Data Portability
It’s all contentious

• 24 hour notification
• Maximum fines of up to 5% of world wide turnover or 100 million Euros
• All countries will have to comply
• Safe Harbour Rules
• Single authority for companies operating in multiple countries
Security?

• Confidentiality – do we really have this one sewn up?
• Integrity – will become far more important when there is so much data to prove that you were doing wrong. Yet if you can’t secure this data, you were always doing wrong
• Availability – The data that is being collected with the purpose of making it available to ever more people and organisations than ever
• So, what of security in an open data world?
Concluding thoughts

- Instil good Data Governance into your organisations
- Your organisation should understand what data it would like to hold, why it would like to hold that data in terms of processing, and then make all this clear to users
- Delete / anonymise data after a reasonable period of time if you intend to continue using it for profiling
- Understand where your data comes from, where it goes to, and is shared with, then make that clear in your privacy statements
- Make things easy for your users and for yourselves
- Protect the rights of your users as if they were your own
- Ask, how would I, my partner, children, parents, friends, relatives feel if they knew we were doing this with their data?
- Remember, people only care when it gets personal
- Don’t get personal with other peoples data rights
Questions?

sarbs@incomingthought.com
Benefits for citizens

- A right to be forgotten
- Easier access to your own data
- Allowing you to decide how your data is used
- The right to know when your data has been hacked
- Data protection first, not an afterthought

The information on this and the remaining slides are from a speech given by Vice-President Viviane Reding, the EU's Justice Commissioner said ahead of data protection day on 27th January 2014. It is available from: http://europa.eu/rapid/press-release_MEMO-14-60_en.htm
Benefits for business

• One continent, one law
• One-stop-shop
• The same rules for all companies – regardless of their establishment
• European regulators will be equipped with strong enforcement powers
Benefits for SMEs

• Exempt to appoint Data Protection Officers
• No more notifications
• Where requests to access data are excessive or repetitive, SMEs will be able to charge a fee for providing access
• SMEs will have no obligation to carry out an impact assessment unless there is a specific risk
What is the EU response to allegations of surveillance of European citizens by US intelligence agencies?

• A swift adoption of the EU's data protection reform
• Making Safe Harbour safer
• Strengthening data protection safeguards in the law enforcement area
• Use the existing Mutual Legal Assistance and Sectoral agreements to obtain data
• Addressing European concerns in the on-going U.S. reform process
• Promoting privacy standards internationally
Making Safe Harbour safer 1

- **Transparency**
  1. Self-certified companies should publicly disclose their privacy policies.
  2. Privacy policies of self-certified companies’ websites should always include a link to the Department of Commerce Safe Harbour website which lists all the ‘current’ members of the scheme.
  3. Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services.
  4. Clearly flag on the website of the Department of Commerce all companies which are not current members of the scheme.
Making Safe Harbour safer 2

• Redress

5. The privacy policies on companies’ websites should include a link to the alternative dispute resolution (ADR) provider.

6. ADR should be readily available and affordable.

7. The Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.
Making Safe Harbour safer 3

• Enforcement

8. Following the certification or recertification of companies under Safe Harbour, a certain percentage of these companies should be subject to ex officio investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements).

9. Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after 1 year.

10. In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority.

11. False claims of Safe Harbour adherence should continue to be investigated.
Making Safe Harbour safer 4

• Access by US authorities

12. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.

13. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.