Information Security Breaches & The Law

Type here and press enter t

- Home
- About »
- "Security Breaches" Library

Article 29 Data Protection Working Party reports on implementation of Data Retention Directive

Posted by "Security Breaches" Administrator on 19/07/2010 · Leave a Comment

I. Background – Enforcement

The Article 29 Data Protection Working Party ("WP29"), comprised of the European Data Protection Authorities ("DPAs"), has adopted on July 13, 2010 a report (the "Report") on the European Union Data Retention Directive 2006/24/EC ("D.R. Directive"). This report is the WP29's contribution to the evaluation of the implementation of the D.R. directive by the European Commission, which is due by September 15, 2010.

National Energy Research Scientific Computing Center's High Performance Storage System (Photo by: Lawrence Berkeley Nat'l Lab - Roy

Kaltschmidt, 2009)

The report details the results of a joint inquiry made by the DPAs about the compliance, at the national level, with the obligations of telecom providers and Internet service providers (the "providers") with both the D.R. directive and articles 6 and 9 of the EU e-Privacy Directive 2002/58/EC ("e-Privacy Directive").

Indeed there is a tension between the e-Privacy Directive and the D.R. Directive. Article 6 (1) of the e-Privacy Directive provides that

> "*traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.*" Traffic data can only be stored for the purpose of billing the customer and interconnection payments, and only "*up to the end of the period during which the bill may lawfully be challenged or payment pursued.*" (article 6(2) of e-Privacy Directive)

The D.R. Directive derogates from the e-Privacy Directive's provisions, as its objective is to

> "*harmonise Member States' provisions … with respect to the retention of certain data which are generated or processed by [electronic communications services or of public communications networks], in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.*" (article 1(1) of the DR directive)

Data retention has a significant impact on the security of the stored data. However, the joint inquiry found out that the D.R. Directive is not applied correctly by providers. WP29 called for "*the definition of minimum standards for the security measures to be taken by providers.*" (Report, p.4)

II. Legal Framework

- **Which data are stored?**

Article 5 of the D.R. Directive specifies the categories of data to be retained. Such data are necessary:

• to trace and identify the source of a communication;
• to identify the destination of a communication;
• to identify the date, time and duration of a communication;
• to identify the type of communication;
• to identify user's communication equipment or what purports to be their equipment;
• to identify the location of mobile communication equipment.

- **How long can data be stored?**

Article 6 of the D.R. Directive specifies that data can only be retained "*for periods of not less than six months and not more than two years from the date of the communication.*"

- **Data security principles**

Article 7 of the D.R. Directive specifies the following data security principles that must be followed, as a minimum:

> *"(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;*
>
> *(b) the data shall be subject to appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure;*
>
> *(c) the data shall be subject to appropriate technical and organizational measures to ensure that they can be accessed by specially authorized personnel only; and*
>
> *(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention."*

Each Member State must designate a public authority responsible for monitoring the application within the State of these security principles (article 9 of D.R. Directive). However, these principles are "*to be regarded as the minimum level to be afforded by each MS*." (Report, p. 5)

III. Enforcement Action

- **Data Security Risks**

> "*Under directives 2006/24/EC and 2002/58/EC, the security of personal data must be proportionate to the risks arising from the processing of such data and the features of the data.(…) It is unquestionable that the implementation of the D.R. Directive carries specific risks to data subjects on account of the nature of traffic data.*" (Report, p. 6)

Because data may be negligently retained, leading to unauthorized disclosure or access to this data,

> "*implementation of the D.R. Directive by electronic communications and Internet service providers is associated with an inherently high risk level such as to require appropriate technical and organisational security measures.*" (Report, p. 6)

- **Methodology**

DPAs answered a questionnaire which included questions addressing the technological solutions implemented for retention purposes, such as IT security, logical protection, authentication/authorisation, logs, encryption, disclosure/transmission protocols, physical protection, and back-up/disaster recovery. (Report, p.7)

- **Findings**

The answers showed that security measures had been applied on a piecemeal basis, and some were even found to be inaccurate or imprecise, which lead to ad-hoc sanctions and specific technical and

organizational measures. (Report, p.8)

WP29 called for preventing that the enforcement activities of DPAs be limited

> "*by possible constraints, including those related to business/industry confidentiality, where such constraints may be relied upon by the said providers in order to not disclose the requested information. It is necessary to give broad enforcement powers to DPAs, including the power to demand access to business/industry confidentiality.*" (Report, p. 8)

- **Retention Periods**

Data may be potentially detained for 6 to 24 months. Data is retained in Member States for 12 months (48%), for more than 12 months (30%), and for 6 to 12 months (22%). (Report, p.10)

Data in law enforcement-accessible systems are sometimes stored in others systems before hand, and are thus accessible within the providers' organisation. WP29 calls for the Commission and other institutions in charge of assessing operation of the D.R. Directive

> "*to take into account the overall sensitivity of traffic per se and reconsider their overall security – regardless of whether such data is stored in systems and for purposes other than those referred to in the D.R. Directive*" (Report, p.11)

Indeed, allowing different security levels and retention periods based on whether systems contain traffic data as mentioned in the D.R. Directive, or merely contain traffic data used for business-related purposes would "*mean lowering the overall security of the traffic data and failing ultimately to meet the requirements made by the D.R. Directive – i.e. that traffic data should be retained for limited periods and accessed on the basis of specific constraints.*" (Report, p. 11).

- **Technical and Organizational Security Measures**

Article 7(b) of the D.R. Directive requires that retained data be subject "*to appropriate technical and organizational measures*" in order to protect its integrity and security. The D.R. Directive does not require additional security measures than the ones provided for by the e-Privacy Directive and the D.P. Directive.

However,

> *"the risk level associated with traffic data per se mandates strict, risk-adjusted security standards to be implemented by having regard to the nature of such data, the amount of stored data, and the retention periods.*"

It was found that providers' awareness of the risks associated with telephone and Internet traffic data was reflected in the security measures they had implemented. Instead, they must be provided with detailed guidance so they can prevent taking inadequate security measures. (Report, p. 11)

In order to detect all the relevant risk factors, providers should regularly and objectively assess risks associated with traffic data. They should pay special attention to access control and data availability.

Regular external audits could also objectively assess risks. (Report, p.11) Only 45% of the companies rely on external audits or third party security certifications. (Report, p. 12).

Compliance with technical and organizational security obligations is not consistent, and security measures vary with the provider's business size. Small providers have lower security standards and are unable to implement optimal security measures because of the cost of implementing them. Indeed,

> *"not all the systems processing traffic data for commercial purposes were designed or implemented by keeping in mind the need to ensure adequate security levels for traffic data. There appears to be no standard awareness of the risks related to traffic data retention*." (Report, p. 12)

Traffic data is by nature very sensitive and should thus be treated in a way comparable to the categories of data mentioned by article 8 of the European Union Directive 95/46/EC (Data Protection Directive, or "D.P. Directive"), which prohibits processing of sensitive data such as political opinions, sexual orientations, or ethnic origins. Retention of such data should be "*adapted to their sensitive nature*," and "*extra attention is required as to their access by, and onward transfer to, the LEAs [law enforcement authorities].*" The Article 29 WP recommends that "*the conditions for access and onward transfer of retained data should be clearly specified in the law*." (Report, p. 13)

Self-regulation is not enough, "*primarily because of the uneven balance of power between the service providers (…) and the LEAs.*" The WP29 makes the following suggestions which can be implemented to ensure that data may only be accessed by duly authorised staff pursuant to Article 7(c) of the D.R. Directive :

- strong access control to the retained data:

- definition of user responsibilities;
- profiles with different user privileges

- **strong authentication for system access:**

- dual authentication mechanisms, (i.e. password + biometrics, or password + token)

- **detailed tracking of accesses and processing operations:**

- log retention

- **log integrity**:

- encryption technology or equivalent measures

- **logical separation from other systems processing traffic data for commercial purposes**

- **additional necessary measures:**

- detailing roles and functions of system administrators dealing with systems where

traffic data are stored for LEA-related purposes
- ad-hoc policy documents

The WP29 also recommends using third party certification programs: providers could thus implement more easily security measures applying to traffic data, and they could incorporate both in-house policies and *strictu sensu* technological measures in a security certification programme. Such programme should be run regularly, preferably by an external third party, and should respect internationally agreed standards. (Report, p. 13)

DPAs should also be able to carry out audits or audits should be made available to them. (Report, p. 13)

Article 7(d) of the D.R. Directive provides for an exception applying to retention of the data accessed by LEAs. These data can disclose important, sometimes sensitive information on users. However, they may be stored *de facto* for an indefinite additional period. Additional security measures specifically targeting this category should be provided, even though no specific requirements are laid down in the D.R. Directive. (Report, p.14)

- **Handover Procedures**

Handover procedures applying to the traffic data requested by LEAs is not homogeneous, as a wide range of procedures, from e-mail or fax to encryption, is used to transmit these data. WP29 recommends developing a standard IT procedure. Doing so would "*significantly enhance the overall security level of the handover procedure*," by ensuring its integrity, confidentiality, and non-repudiation. (Report, p. 15)

For instance, such procedures should provide for mutual authentication, connections should be encrypted, and the communication channels should be trusted and secured based on key and digital signature certificate exchanges. (Report, p. 15)

Pan-European handover standards could include a single contact point at each service provider, and a single data handover format, which would include fields allowing a secure, interchange/access between stakeholders (Report, p. 15) Doing so would also minimize some issues arising from the fact that LEAs pressuring providers for acquiring user-related data not listed in the D.R. Directive, or submitting access requests without formal warrants, or unauthorized (i.e. non-LEA) entities making access requests. (Report, p. 16).

- **Statistics under Article 10 of the D.R. Directive**

Member States must provide each year the Commission with statistics on the use of retained traffic data (article 10, D.R. Directive). Amendments to the directive should take those statistics into account (article 14, D.R. Directive). Availability of this information is fundamental to assess whether the objective of the Directive are achieved, *"including the need for introducing harmonized principles applying to all EU Member States*." (Report, p. 16).

- **Outsourcing issues**

Outsourcing is frequently used to carry out activities related to traffic data retention, especially among

smaller operators. The data controller may therefore not be able to accurately monitor data processing operations, particularly if data is retained outside domestic borders. Such is the case, for example, with cloud computing systems. Use of outsourcing outside the domestic borders calls for an "*increased level of mutual assistance and cooperation in order to allow access to data and exercise of necessary enforcement powers*." (Report, p. 17) DPAs should analyze this issue in depth, and "*contractual clauses (…) should envisage specific, appropriate security measures*." (Report, p. 18).

IV. Further Actions and Recommendations

Self-regulation alone is not enough because of the uneven balance of power between providers and LEAs. Cost-related issues and competition issues may prevent a self-regulatory approach ensuring high security standards.

- **Retention periods**

The maximum retention period should be reduced, and all EU providers should comply with a single, shorter term. (Report, p. 19)

- **Technical and Organisational Security Measures** (Report, p.20)

1. Providers should regularly and objectively assess the risks associated with traffic data in order to detect risk factors. Special attention should be paid to access control and data availability. Regular external audits could contribute to an independent and objective risk assessment.

2. Additional security measures are suggested :

- strong access control to retained data, by defining user responsibilities and using profiles with different user privileges;

- strong authentication for system access, using dual authentication mechanisms (password + biometrics, or password + token)

- detailed tracking of accesses and processing operations using logs recording at least user identity, access time, and file acceded;

- log integrity using encryption technology;

- separations of processing traffic data for commercial purposes from other systems;

- additional measures as necessary to ensure confidentiality of data.

3. The roles and functions of systems administrators should be detailed in policies, and all the systems maintenance should be controlled in depth.

4. In house policies *and strictu sensu* technological measures should be incorporated in a security certification programme run regularly, preferably by a third party. DPAs may carry out audits or such audits should be made available to DPAs.

5. Accessed data should be deleted in order to respect the provisions of both the D.P. Directive and

international instruments, including Council of Europe's Recommendation R(87)15 regulating the use of data in the police sector.

Marie-Andrée Weiss & Cédric Laurant

Filed under ENGLISH, Outlines · Tagged with sensitive information, EU Directive 95/46/EC, personal data, contractual clauses, European data protection authorities, European Commission, Article 29 Data Protection Working Party, encryption, sensitive personal information, self-regulation, cloud computing, data security, confidentiality, integrity, external audit, EU Data Retention Directive, traffic data, retained data, EU e-Privacy Directive, data security principles, authentication, logs, back-up, password, law enforcement authorities, LEA-accessible systems, technical and organizational security measures, security audit, security certification, security standards, system administrator, security policy, handover procedures, data deletion, access control, biometrics, log retention, third party certification, in-house policies, non-repudiation, mutual authentication, digital signature, warrant, access request, outsourcing, cloud computing system, mutual assistance and cooperation, retention period, dual authentication, tracking, log integrity, system maintenance, Council of Europe Recommendation R(87)15

Are 'clouds' located outside the European Union unlawful?

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <pre> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Post Comment

- [ ] Notify me of follow-up comments via email.
- [ ] Send me site updates

- **Recent Posts**

  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive
  - Are 'clouds' located outside the European Union unlawful?
  - The Safe Harbor Framework: not a "safe harbor" anymore for US companies? German expert body insists on stronger compliance stance
  - Canada May Soon Have a Data Breach Law

- **Recent News on Security Breaches**

  - "Consumer View: Staying Safe from Cyber Snoops" (FCC, June 11, 2010) Recent news reports have focused attention on a growing concern: The ways in which wireless and WiFi networks can make consumers' private data accessible. (…)
  - "Sécurité des données personnelles : les entreprises ne font pas face" (ITR News, 9 juin 2010) L'étude souligne le fait que, en dépit de ce que croient beaucoup d'entreprises, le fait de respecter la réglementation en vigueur ne suffit pas à assurer une protection efficace des données. En effet, alors que 70 % des sondés affirment (…)
  - "Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program" (FTC, June 24, 2010) The FTC's complaint against Twitter charges that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information, tweets that consumers had (…)
  - "UK headed for data breach disclosure law within four years" (siliconcom, July 16, 2010) "According to lawyers at law firm Field Fisher Waterhouse, legislation requiring organisations to notify the relevant authorities as well as individuals affected in the event of a serious security breach will be introduced across Europe."
  - "Survey: 87 per cent of UK businesses favour mandatory disclosure of data breaches" (Secure Business Intelligence, July 6, 2010) 87 per cent of organisations believe that data breaches should be revealed when sensitive data about the public is exposed. Revealed, but to whom?
  - "Putting a Private Detective in Your Laptop" (New York Times, June 16, 2010) "According to a study by the Ponemon Institute, 12,000 laptops are lost each week in American airports (…) You can keep an eye on your devices and not leave them visible and unattended, but they might best be protected with some software."
  - "Credit Card Hackers Visit Hotels All Too Often" (New York Times, July 5, 2010) Hotels are a favorite target of hackers. A study released this year by data-security consulting company SpiderLabs found that "38 % of the credit card hacking cases last year involved the hotel industry".
  - Ponemon Institute: First Annual Cost of Cyber Crime Study (ArcSight, July 26, 2010) "The purpose of this benchmark study is twofold. First, we wanted to quantify the economic impact of a cyber attack. Second, we believed a better understanding of the

cost of cyber crime will assist organizations in determining the appropriate amount (…
  - Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (FTC, July 27, 2010) "The FTC began its investigation following news reports about Rite Aid pharmacies using open dumpsters to discard trash that contained consumers' personal information such as pharmacy labels and job applications. (…)"

- **Tag Cloud**

adequate level of data protection Article 29 Data Protection Working Party Binding corporate rules Bundesdatenschutzgesetz C-29 Canada cloud computing confidentiality contractual clauses damage to reputation data breach notification statute data security Düsseldorfer Kreis encryption EU Directive 95/46/EC European Commission European data protection authorities European Union external audit Facebook German Federal Data Protection Act Germany identity theft integrity material breach online reputation personal data PIPEDA preemption Privacy Commissioner of Canada profile building companies reputation Safe Harbor Framework Safe Harbor self-certification search engines security breach security breach disclosure security breach notification self-regulation sensitive information sensitive personal information significant harm social networking sites TJX United States

- **Blog Authors**
  - 

  - 

- 

- **Disclaimer & Comments Policy**
  - Disclaimer & Comments Policy

- **Authors' upcoming talks & conferences on information security & legal issues**
  - Cédric Laurant: "Seminario internacional: seguridad de la informacion, cibercriminalidad y propiedad intelectual" (international seminar on information security, cybercriminality and intellectual property) IUSTIC & Universidad Pontificia Bolivariana (Medellin, Colombia – Aug. 3-12, 2010)
  - Cédric Laurant: II Congresso Crimes Eletrônicos e formas de proteção (2nd Congress on Cybercrimes and Protection Measures) Federação do Comércio do Estado de São Paulo (Sao Paulo Chamber of Commerce), Sao Paulo, Brazil – Sept. 27-28, 2010
  - Cédric Laurant: "Legal Developments and Relevant Court Decisions in Latin America" High Technology Crime Investigation Association (HTCIA) International Conference (Atlanta, GA-USA – Sept. 20-22, 2010)

- **Tweets (last 10)**
  - List of recent surveys and reports on security breaches: http://bit.ly/9VamhE - tweeted 22 hours ago
  - ArcSight & Ponemon Institute: release of "1st Annual Cost of Cyber Crime Study" http://bit.ly/d1Us8e - tweeted 22 hours ago
  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive. New blog posting at http://bit.ly/aOG3cY #in - tweeted 1 week ago
  - "Are ‘clouds’ located outside the European Union unlawful?" New blog posting. http://bit.ly/djUNCy #in - tweeted 1 week ago
  - "The Safe Harbor Framework: not a 'safe harbor' anymore for US Companies?" New blog posting. http://lnkd.in/ShwMWj - tweeted 2 weeks ago
  - "The Safe Harbor Framework: not a "Safe Harbor" anymore for US Companies?" New blog posting: http://wp.me/pW5Fc-1D - tweeted 2 weeks ago
  - FTC's proposed consent agreement with #Twitter: company misrepresented its security measures. http://bit.ly/cF8LNk - tweeted 1 month ago
  - Your "private" tweets are... public! #Twitter prone to security breaches, FTC says in consent agrmt. Com'ts requested. http://bit.ly/axKpnV - tweeted 1 month ago
  - FTC's 1st case agst social netwkg website: #Twitter failed to safeguard users' PII despite promises in privacy policy http://bit.ly/ajUG9J - tweeted 1 month ago
  - Backing up data is one thing, encrypting the backups another, but restoring the encrypted data, even more complex. http://bit.ly/bGgQt2 - tweeted 1 month ago

- **Subscribe to this blog by e-mail**

  Enter your e-mail address here to subscribe to this blog and receive notifications of new posts by e-mail.

  Sign me up!

-

- **Counters**

- 

Information Security Breaches & The Law ·

Blog at WordPress.com. Theme: Structure by Organic Themes.