WORLD DATA PROTECTION REPORT

Volume 2, Issue 4 April 2002

Monthly news and analysis of data protection & privacy issues from around the World

■ ITALY

Electronic Signatures in Italy (Part I)

By Avv. Alessandro del Ninno, Studio Legale Tonucci, Information and Communication Technology Department, Via Principessa Clotilde n. 7, 00196 Rome, www.tonucci.it, E-mail: adelninno@tonucci.it

With the publication in The Italian Official Journal of the Legislative Decree of January 23, 2002 No. 10 "*Implementation of the EU Directive 1999/93/EC on a Community framework for electronic signatures*", Italy has introduced new rules on electronic signatures to comply with the EU Directive. Considering that in Italy electronic signatures have been fully valid since 1997, it may be useful to shortly illustrate the previous Italian legal framework on the matter, before the carrying out of an in-depth analysis of the new rules and the related modifications.

Previous Legal Framework on Electronic Signatures

In 1997, Italy enacted the first European law about the validity of electronic signatures: the Presidential Decree No. 513 of 10 November 1997 "*Regulations establishing criteria and means for implementing Section 15(2) of Law No. 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems*".

Law No. 59 of 15 March 1997 "*Delegation of powers to the Council of Ministers to confer tasks and functions on Regions and local authorities, to pursue the reform of the public administration, and to simplify administrative procedures*", provided that acts, data and documents created by Public agencies and private persons by means of computer-based or telematic systems, contracts drawn up by such means, as well as their storage or transmission by means of computer systems, shall be legally valid and relevant for any purpose of law (article 15).

The provisions contained in the mentioned Decree 513/1997 have been successively inserted in the Presidential Decree of December 28, 2000 No. 445 "*Consolidation Act related to the legislative and regulation provisions about administrative documentation*". Consolidation Acts represent a particular legislative technique: all the legislative and regulation provisions on a certain matter, spread over several acts, are collected in an unique text.

In particular, before the entering into force of the new Legislative Decree No. 10/2002, the Consolidation Act 445/2000—Section V, articles 22-29 contained the current discipline in force about electronic signatures.

Main Concepts of Electronic Signatures

According to the Consolidation Act 445/2000, the main concepts related to electronic signatures in Italy are the following:

"*Electronic document*" the computer-based representation of legally relevant acts, facts or data.

"*Digital signature*" means the result of a computer-based process (validation) implementing an asymmetric cryptographic system consisting of a public and a private key, whereby the signer asserts, by means of the private key, and the recipient verifies, by means of the public key, the origin and integrity of a single electronic document or a set of such documents; (the previous Italian rules made a distinction between "electronic" and "digital" signatures, being a "digital signature" the one as defined in the Consolidation Act 445/2000).

"*Validation system*" means a computer-based cryptographic system capable of creating and affixing digital signatures or of verifying the validity of digital signatures.

"*Asymmetric key*" means a pair of cryptographic keys comprising a public and a private key, related to each other, to be used of the encryption or validation of electronic documents.

"*Private key*" means the item within an asymmetric key pair, that is meant to be known only to the holder of

the asymmetric keys, and that is used to affix a digital signature to electronic documents or to decrypt electronic documents previously encrypted by means of the corresponding public key.

"Public key" means the item, within an asymmetric key pair, that is meant to be made public and that is used to verify the digital signature affixed to electronic documents by the holder of the asymmetric keys, or to encrypt electronic documents for transmission to the holder of the asymmetric keys.

"Biometric key" means a string of computer-based codes used in security systems that verify personal identity by reference to physical features unique to the user.

"Certification" means the result of a computer-based process that is applied to the public key and that can be detected by validation systems, whereby the public key is certified unique to its holder, the holder is identified, and the period of validity of the key and the expiry date of the corresponding certificate are set, for a period not exceeding three years.

"Validation by time-stamp" means the result of a computer-based process under which one or more electronic documents are marked with a date and time that are legally valid against third parties.

"Electronic address" means the identifier of a logical or physical resource that is capable of receiving and recording electronic documents.

"Certification authority" means the public or private entity that effects the certification, issues the public key certificate, makes the public key and the corresponding certificate publicly available, and publishes and updates certificate "

"Revocation of a certificate" means the permanent invalidation of a certificate by the certifying authority as from a specific point in time, excluding retroactive invalidation.

"Suspension of a certificate" means the temporary invalidation of a certificate by the certifying authority.

"Validity of a certificate" refers to the fact that the information recorded in a certificate is legally valid and invocable against the holder of the corresponding public key.

"Technical rules" means technical specifications, including any legal provision to be applied to them.

Rules Relating to Digital Signatures

A digital signature may be affixed or associated by means of a separate document to any electronic document, set of electronic documents, on copies or duplicates thereof.

Affixing a digital signature to an electronic document or associating one with it shall have the same effects as putting the required signature to acts or documents written or paper.

Any digital signature must uniquely identify a single entity and the document or documents to which it has been affixed or with which it has been associated.

The private key used to generate a digital signature must correspond to a public key that is still within its period of validity and that has not been revoked or suspended by the public or private entity that carried out the certification.

Using a digital signature affixed or associated by means of a revoked, suspended or expired key shall have the same effects as failure to sign. Revocation and suspension, whatever the reason, shall take effect on the moment of publication, unless the revoking authority or the entity requesting suspension proves that revocation or suspension was already known to all interested parties.

Affixing a digital signature shall, for all purposes in law, complement and substitute for any required seal, stamp, countersign or other distinctive mark.

By means of the methods and techniques specified in the Prime Minister Decree of February 8, 1999 *"Technical rules for the setting up, sending, recording, reproducing, duplication, validation of electronic documents as per art. 3 of the Presidential Decree of November 10, 1997 No. 513"*, a digital signature must disclose such elements as are sufficient to identify the subscriber, the authority that carried out the certification, and the repository where it is accessible for consultation.

Authenticated Signatures

A specific kind of digital signature is represented by the *"authenticated digital signature"*. The digital signature authenticated by a notary public or another authorised public official shall be deemed to be an authenticated signature for the purposes of Section 2703 of the Italian Civil Code. Article 2703 cc. (*Authenticated signature*) provides that a signature that has been authenticated by a notary or by another authorised public official is treated as having been recognised. The authentication consists of a certification by the public official that the signature was written in his presence. The public official must previously verify the identity of the person who makes the signature.

In order to authenticate a digital signature, the public official shall certify that the digital signature was affixed by the signer in the presence of the official following verification of the signer's identity and the validity of the public key; that the signed document reflects the signer's will, and that it is not in breach of existing laws.

The public official's digital signature shall, for all purposes in law, complement and substitute for any seal, stamp, countersign or other distinctive mark that may be required.

Where an electronic document must be accompanied by another document originally created on a different medium, the public official may attach a certified true electronic copy instead.

Digital signatures inserted into electronic documents delivered to or deposited with a Public agency shall be regarded as having been affixed in the presence of the responsible agent.

Documents delivered to or deposited with a Public agency over telematic systems or on a computer-based medium shall be valid, for all purposes in law, on condi-

tion that they have been digitally signed and validated by time-stamp.

A digital signature shall substitute for a hand-written or otherwise required signature in all electronic documents of Public agencies. The use of a digital signature shall, for all purposes in law, complement and substitute for any required seal, stamp, countersign or other distinctive mark.

The holder of an asymmetric key pair may deposit the private key under secrecy with a notary public or another authorised public repository.

The private key to be deposited shall be recorded on any suitable medium by the owner. It shall be delivered in a sealed package such that the information recorded cannot be read, extracted or be otherwise made known without causing alterations or breakage.

Any person or entity intending to utilise, an asymmetric cryptographic system shall obtain a suitable key pair. One of these keys shall be made publicly available by means of the certification process carried out by a certifying authority.

Public keys shall be kept by the certifying authority for at least 10 years from the date of publication. They shall be accessible by telematic means as from the beginning of their period of validity.

Certifying Authorities

Without prejudice to the provisions related to the Public Agencies, the certification operations shall be conducted by certifying authorities named, following notification prior to the beginning of operation, in a public list accessible by telematic means. The list shall be drawn up, maintained and updated by the AIPA. Certifying authorities shall fulfil the following requirements, further specified in the Prime Minister Decree of February 8, 1999 "*Technical rules for the setting up, sending, recording, reproducing, duplication, validation of electronic documents as per art. 3 of the Presidential Decree of November 10, 1997 No. 513*".

Certifying authorities that are private entities shall be set up as joint-stock companies; their registered capital shall meet at least the working capital requirements for authorised banking enterprises (which is EUR 6.455.000 - ITL 12.500.000.000).

Legal representatives and administrators of certifying authorities shall meet the requirements of good repute laid down for persons in executive, managerial or auditing positions in banks.

Assurance must be given that the certifying authority's responsible technical staff and staff charged with carrying out certification procedures are sufficiently knowledgeable and proficient to satisfy the provisions set out in this regulation and the technical rules of the Decree of February 8, 1999. The quality of computer-based processes and products shall meet internationally recognised standards.

The certification process above mentioned may also be carried out by a certifying authority whose license or authorisation was issued, subject to equivalent requirements, by another member State of the European Union or European Economic Area.

Any person or entity intending to make use of an asymmetric key or digital signature system shall take all necessary organisational and technical measures to prevent loss or damage to third parties.

The certifying authority shall:

- Accurately identify the person applying for certification;
- Issue and publish certificates meeting the requirements to be set out in the Decree of February 8, 1999;
- On request of the subscriber, and with the assent of the third party concerned, specify any Power of representation or other title relating to the subscriber's profession or office held.
- Meet the technical rules contained in the Decree of February 8, 1999;
- Provide exhaustive and clear information to the applicants concerning the certification practice and the technical requirements necessary to obtain certification;
- Comply with provisions concerning the minimal security standards of computer systems and the treatment of personal data, according to Section 15 (2) of Law No.675 of 31 December 1996;
- Not accept the deposit of private keys;
- Promptly revoke or suspend certificates in the following circumstances: on request of the subscriber or of the third party of whom the subscriber is an authorised agent; in case the key has been compromised; on decision of an authority; on disclosure of facts limiting the subscriber's capacity; if abuse or forgery is suspected;
- Immediately make public any revocation or suspension of an asymmetric key pair;
- If the certification activity is discontinued and records are consequently invalidated or transferred to another certifying authority, immediately notify the AIPA and the subscribers, at least six months in advance.

In accordance with their statutes, Public agencies shall, on their own authority, generate, store, certify and use their own public keys.

The public keys of public officials not employed in Public agencies shall be autonomously certified and published, in accordance with the relevant laws and regulations governing the use of hand-written signatures. Public keys held by legally recognised Professional registers and or their legal representatives shall be certified and published by the Ministry of Justice or by delegated agents.

Having analysed in detail the previous Italian legal framework on electronic signatures, it is important to illustrate and to compare the new provisions on Electronic Signatures introduced by the Legislative Decree 10/2002: the related analysis will be published in Part 2 of this article in the next issue.

Electronic Signatures in Italy (Part 2)

By Avv. Alessandro del Ninno, Studio Legale Tonucci, Information and Communication Technology Department, Via Principessa Clotilde n. 7, 00196 Rome. See www.tonucci.it; E-mail: adelninno@tonucci.it

Legislative Decree of January 23, 2002 No. 10 introduces relevant modifications, especially if compared with the rules of the Consolidation Act No. 445/2000 (which shall continue in force). In any case, the Legislative Decree 10/2002 provides that within 30 days starting from its entering into force (March 2, 2002), a specific Regulation to co-ordinate the new provisions with the ones contained in the Consolidation Act 445/2000 must be enacted. With this Regulation shall be specified also the new requirements for the certification service providers.

First of all, it can be useful pointing out the different definitions of the legal terms contained in article 2 of the Legislative Decree 10/2002, especially if compared with those of the Consolidation Act 445/2000 above illustrated (and which are still in force with specific regard to that kind of electronic signatures defined as "advanced electronic signature" in the new Decree).

According to article 2:

"electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as an informatic method of authentication;

"certification-service-provider" means an entity who issues certificates or provides other services related to electronic signatures;

"credited certification-service-provider" means certification service providers credited in Italy or in other Member States of the UE according to article 3, paragraph 2 of the EU Directive 1999/93/EC (Article 3, paragraph 2 provides: "without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive");

"electronic certificates" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

"qualified certificate" means a certificate which meets the requirements laid down in Annex I of the UE Directive 1999/93/EC and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II.

Requirements for Qualified Certificates

With regard to the requirements laid down in Annex I and II of the EU Directive 1999/93, it is useful to fully report the related texts:

EU Directive 1999/93/EC - ANNEX I:

Requirements for qualified certificates

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification of the certification-service-provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond to signature-creation data under the control of the signatory;

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification-service-provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable; and

(j) limits on the value of transactions for which the certificate can be used, if applicable.

Certification Service Providers

EU Directive 1999/93/EC - ANNEX II:

Requirements for certification-service-providers issuing qualified certificates.

Certification-service-providers must:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes;
- information can be checked for authenticity;
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained; and
- any technical changes compromising these security requirements are apparent to the operator.

Other Legislative Definitions

Carrying on the analysis of the provisions contained in article 2 of the Legislative Decree 10/2002, the other legislative definitions are:

"secure-signature-creation device" means a signature-creation device which meets the requirements laid down in article 10; (see infra pp. 30-31)

"advanced electronic signature" means an electronic signature which meets the following requirements:

1. it is uniquely linked to the signatory;
2. it is capable of identifying the signatory;
3. it is created using means that the signatory can maintain under his sole control; and
4. it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

"voluntary accreditation" means the recognition of the certification service provider's possession of the requirements set up at the highest level in terms of quality and security, provided that the certification service provider requires such recognition.

Appointment of Certification Providers

One of the most important new provisions is related to the new system of appointment of certification service providers. The Legislative Decree provides that the certification activity carried out by a certification service provider in Italy or elsewhere in the EU territory is free (article 3). No preventive authorisation is required. It is only requested (article 4) that, before the beginning of his activity, the certification service provider who wants to issue qualified certificates shall communicate—even by means of telematic devices—the starting of the activity to the Department of Innovation and Technology of the Council of Ministries' Presidency (entity which shall carry on control and supervision activities with regard the whole sector on the basis of notices coming from public or private subjects or "ex officio"). Before the new discipline, as illustrated above, the rules in force required particular conditions to comply with.

Further, with the new Legislative Decree a special "optional accreditation system" for certification service providers is also introduced (article 5). Certification service providers can optionally request to the Department of Innovation and Technology of the Council of Ministries' Presidency to be recognised as certification authorities which comply with the highest requirements in terms of quality and security of the service. If the certification service provider so requires, he shall have to demonstrate the possession of additional technical requirements (additional requirements with regard to the basis requirements of the certification service providers who supply non-qualified certificates). Moreover, he shall demonstrate the possession of requirements of honour and a financial soundness. If the Department of Innovation and Technology of the Council of Ministries' Presidency shall accept the application, the appointed certification service provider shall be inserted in a special list held by the Department itself and publicly available also by means of telematic devices. In any case, it must be pointed out that a specific further Regulation to be still enacted shall clarify in detail the particular requirements to be held by the certification service providers.

Form and Efficacy of Documents

A very important provision is contained in article 6 of the Legislative Decree 10/2002. This provision, in fact, modifies in part article 10 of the Consolidation Act 445/2000 with regard to the form and efficacy of electronic documents. It is provided that electronic documents shall have the evidential weight provided for under Section 2712 of the Civil Code with regard to the facts and the things represented. Article 2712 of the Italian Civil Code (Mechanical reproductions) provides that photographic or cinematographic reproductions, phonographic recordings and, in general things, constitute full evidence of the facts or things represented, if the persons against whom they are offered do not deny their correspondence to the actual facts or things concerned.

Further, electronic documents signed with an electronic signature shall have the evidential weight of a private deed. With regard to its evidentiary value, the electronic document itself shall be freely evaluated, according to its objective characteristics in terms of quality and security. Further, it shall satisfy the requirements referred to in Sections 2214 et seq. of the Italian Civil Code

or in any other equivalent statutory or regulatory provision. Art. 2214 Civil Code (Mandatory books and other commercial books) provides that:

> "the enterpriser who exercises a business activity shall keep a journal and an inventory book. He shall, moreover, keep other accounting records required by the nature and size of the enterprise, and preserve in on orderly manner for each transaction the originals of the letters, telegrams, and invoices sent out. The provisions of this paragraph to not apply to small enterprisers according to article 2083 cc".

The new text of article 10 of the Consolidation Act 445/2000 as amended by the Legislative Decree 10/2002 now provides the distinction between "electronic signature" and "advanced electronic signature", called "digital signature". It is provided that the electronic document, when signed with a digital signature (which was the only kind of signature previously provided in the Italian Laws) or with any other kind of advanced electronic signature, and the digital signature is based on a qualified certificate and created by means of a secure-signature-creation device, then the electronic document fully stands up in court (unless an action for false is brought) with regard to the provenance of the declarations made by the subject who has signed the electronic document itself.

Juridical Effectiveness

On the other hand, when an electronic document in signed with an electronic signature (so not by means of an advanced or digital signature), in any case it shall be prohibited to deny full juridical effectiveness and efficacy to that document and to refuse its admissibility as evidence in legal proceedings only according to the fact that the document is signed with a signature not based on a qualified certificate or on a qualified certificate released by a credited certification-service-provider, or—finally—because the signature has not been affixed using a secure-signature-creation device. The provisions above mentioned shall apply also when certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country not belonging to the European Union. In this case, the certificates are recognised as legally equivalent to certificates issued by a certification-service-provider established within the EU if:

- the certification-service-provider fulfils the requirements laid down in the EU Directive 1999/93/EC and has been accredited in a Member State; or
- a certification-service-provider established within the EU which fulfils the requirements laid down in the Directive1999/93/EC guarantees the certificate; or
- the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the EU and third countries or international organisations.

Liability for Damages

Another modification introduced is about the liability of certification service providers (article 7). By amending article 28 of the Consolidation Act 445/2000, it is now provided that when a certification service provider who issues certificates as qualified certificates to the public or guarantees certificates to the public, he shall be liable for damages (unless the certification-service-provider proves that he has not acted negligently) caused to any entity or legal or natural person who reasonably relies on that certificate:

- as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
- for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
- for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both.

Article 7 of the Legislative Decree 10/2002 also provides that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate, provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damages arising from use of a qualified certificate which exceeds the limitations placed on it.

A certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties. The certification service provider shall not be liable for damage resulting from this maximum limit being exceeded.

Article 9 of the Legislative Decree 10/2002 substitutes article 38, paragraph 2 of the Consolidation Act 445/2000 with a new version. The previous version of paragraph 2 only provided a general obligation to use a digital signature or the electronic identity card. It is now provided that the applications and the declarations sent by means of telematic devices are fully valid if:

- signed with a digital signature based on a qualified certificate released by a credited certification service provider and created by means of a secure-signature-creation device;
- when the author is identified by the electronic system by using the electronic identity card or the National Card of Services.

Specific Rules Introduced

The Legislative Decree 10/2002, beyond introducing a new discipline in the field of electronic signatures, also provides specific rules about the electronic identity cards and the new National Card of Services which Italy—one of the first countries of the world—is near to introduce within 2002, even if the specific analysis of the related provisions is not carried out in this article, focused on electronic signatures.

Further, the conformity of secure signature-creation-devices with the requirements laid down in Annex III of the EU Directive 1999/93/EC shall be determined based on the so called National Scheme for the Evaluation e Certification of Security in the field of Information and Communication Technology, which will be set up by a Decree enacted by the Prime Minister or by the Minister of Innovation and Technology delegated by the Prime Minister. Such Decree shall designate the appropriate public body which shall credit the evaluation centres and shall certificate the security evaluations. It is also provided that the National Scheme for the Evaluation e Certification of Security in the field of Information and Communication Technology could provide additional European and international criteria for the evaluation and the certification related to other systems or products of the ICT sector.

Finally, It must be pointed out that the Legislative Decree 10/2002 provides that, with regard to the tax fulfilments related to electronic documents, the Ministry for Economy and Finance shall enact a specific Ministerial Decree to clarify the modalities.

Legal Sources and Legislative Texts (in Italian)

Legislative Decree of January 23, 2002 No. 10 "Implementation of the EU Directive 1999/93/EC on a Community framework for electronic signatures". *www.camera.it/parlam/leggi/deleghe/teste/02010dl.htm*

Presidential Decree of December 28, 2000 No. 445 "Consolidation Act of legislative and regulatory provisions about administrative documents". *www.interlex.com/testi/dpr00445.htm*

Prime Minister Decree of February 8, 1999 "Technical rules for the setting up, sending, recording, reproducing, duplication, validation of electronic documents as per art. 3 of the Presidential Decree of November 10, 1997 No. 513". *www.interlex.com/testi/regtecn.htm*

Circular CR/22 of July 26, 1999 (published in the Italian Official Journal of August 2, 1999 No. 179). *www.aipa.it/servizi[3/nromativa[4circolari]2/aipacr22.asp*

Circular CR/24/2001 "Guidelines for the Interoperability of Digital Signatures Certification Service Providers". *www.aipa.it/attivita[2/gruppi[2/index.asp.*

INTERNATIONAL BNA

WORLD DATA PROTECTION REPORT

Volume 2, Issue 5 May 2002

Monthly news and analysis of data protection & privacy issues from around the World