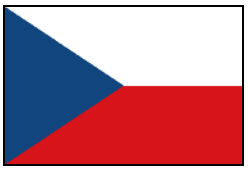




Manual
on Data Protection in E-Communications

Conducted in the framework of the
Twinning Light Project Czech Republic – Austria
"Assistance to the Office for Personal Data Protection
in Exercising Supervision in Personal Data Protection"

(CZ04/IB/OT/02 - TL, CZ2004/006-237/04.06.01.0001)

written by
Lukas Gundermann, Marcus Hild, Bernhard Karning

November 2006

Ludwig Boltzmann Institute of Human Rights, Vienna

Mandated Body

About the authors:

Lukas Gundermann is Head of Division at the Independent Centre for Privacy Protection, Kiel, Germany.

Marcus Hild works as an Officer at the eGovernment Register Authority of the Austrian Data Protection Commission, Vienna, Austria.

Bernhard Karning is Deputy Head of the Department of E-Government - Legal, Organisational and International Issues at the Federal Chancellery of the Republic of Austria, Vienna, Austria.

This publication was produced with the assistance of the European Union. The contents of this publication lie within the sole responsibility of the project partners and can in no way be taken to reflect the views of the European Union.

List of Content

1 Different roles in a prototypic internet service

From a conceptual viewpoint, basically four different roles can be identified with regard to the services provided on the Internet (see figure 1):

- the user,
- the Internet Access Provider (IAP),
- the Internet Service Provider (ISP) and
- the content provider.

Although these roles can be distinguished sharply in theory, it should be borne in mind that the picture developed here is chiefly a prototypic concept. In reality, several of the actors mentioned play more than one role; e.g. companies providing access to the internet frequently offer other services like web hosting, e-mail services and a portal site containing information and links to other websites. Also a person playing the part of a user can at the same time easily be a provider of services in a different surrounding, for example offering some web content of his own.

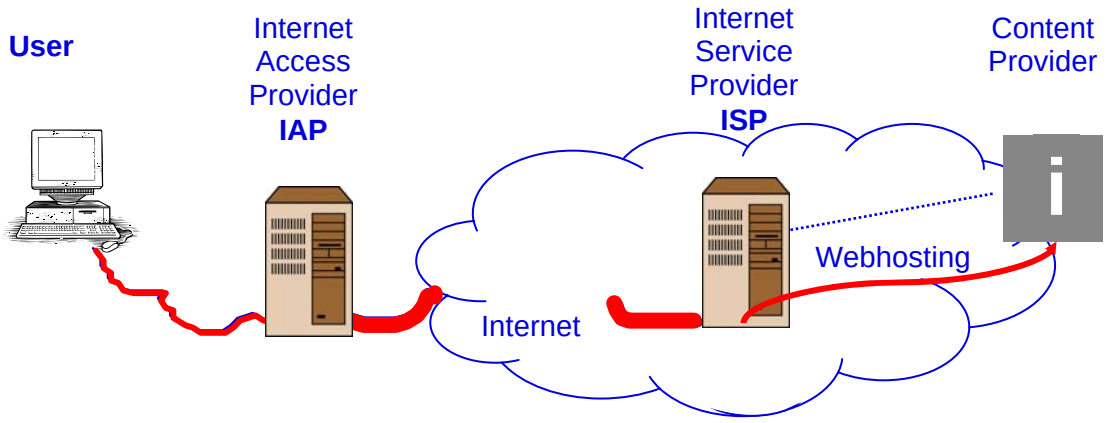


Figure 1: Prototypical roles in the context of Internet use

1.1 User

According to the model developed here, the user is accessing the internet from a location different from the provider's facilities. Independent from the underlying technology, be it a modem, a terminal adapter (ISDN), an ADSL connection, access via mobile phone etc., it is necessary for the user to agree with the IAP on a contractual basis in order to gain access via the technical infrastructure the IAP provides. Therefore, in many cases a written contract is

concluded between the user and the IAP, containing in many cases also the particulars of the user. However, different business models exist, as e.g. dial-in on a call-by-call basis.

The request of any kind of information by the user as well as the delivery by any service create a great amount of so called traffic data which contain information on the communication processes, even if the content itself is not being revealed. This results from the fact that not only the servers of the IAP are handling such traffic data, but all computers at every hub where the conveyed data packages are passing throughout the net. Therefore, from a data protection perspective, the main concern with a view to the user is the collection and usage of traffic data. However, the user himself might also utilise the internet for the processing of personal data such as sending personal data to other recipients or collecting personal information freely available on the internet.

1.2 Internet Access Provider

The business model of the Internet Access Provider is based on the provision of basic services which enable the users to access the internet. Apart from allocating an IP number to the user for the time he or she accesses the internet (for more details see below), the IAP provides connectivity by connecting users to the regional internet backbones and by undertaking to route the users data packages through the net.

The IAP could also be described as the bottleneck where all data stemming from or destined for the user has to pass through. Thus, on a technical level, he is capable of intercepting the users e-communication. Being in this unique position, he might be approached by law enforcement agencies intending to exercise lawful interception of e-communication. The legal regime governing business activities will be changing dramatically after the new Directive on data Retention 2006/24/EC is transposed into national law.

1.3 Internet Service Provider

As mentioned above, the Internet Service Provider (ISP) can not always be strictly separated from the IAP in practice. Many companies in the market are pursuing both business cases and offer even more services such as e-mail in addition. Moreover, the terminology is not consistent, sometimes using ISP as generic term, including IAP. However, in order to provide at least a stringent theoretical approach, the term ISP shall be reserved in this paper for services that run servers on the internet in order to store and make available certain information (although not necessarily for the public). This applies to both, web hosting services and e-mail providers.

Even though these services are different in terms of technical features and the details of their business (the e-mail provider is storing conveyed content protected against unauthorised access, the web hosting service mainly publishing content on a behalf of the content provider), there is a technical feature they have in common: ISPs are maintaining servers which are equipped to log all traffic data and store it as protocol data. In particular at web servers, by

default reports or log files are systematically being recorded that contain all or some of the data that are being conveyed together with each request for information on a technical basis (such as the IP address, type of browser used, etc.).

1.4 Content Provider

The content provider can be an individual or an organisation such as a public institution (e.g. a public authority) or a company rendering information or trying to promote goods or services on a website. Normally, the website is hosted by an ISP, which means that the person or institution responsible for the website rents storage capacity on a web server from an ISP for storing the website and making it available on the internet.

It goes without saying that the content provider bears responsibility for the content and is the one to be held liable for any possible infringements caused by it. In many cases, the content provider is being furnished with statistics of the usage of the web page by the ISP. From a data protection perspective, it is of interest, whether the data provided to the content provider contain any data linkable to an individual.[1] In a more complex model, the service contract between the ISP and the content provider could include the provision of more specific applications on the internet, e.g. a shopping module. In such cases, data related to the customers' business transactions would be transferred to the content provider. In terms of data protection, it will be of interest whether the content provider receives more data about the usage of the web site than are actually necessary for the execution of the contract with the user (such as click stream data).

1.5 General remark

More types or subtypes of service providers could be classified on different layers, providing more specific services. However, at this stage, the four roles involved in a typical process should be sufficient to illustrate the most important data protection concerns. Nevertheless, when dealing more in detail with specific services, other roles and sub-roles will be analysed in addition.

It should be noted, too, that the scope of this paper is focused mainly to conveyance of data which could be referred to as e-communications in a narrower sense. The services of 'classic' telecommunications provider are mostly outside the scope. Those services will mainly be used to connect the user to the IAP. Dir 2002/58/EC is imposing certain obligation on them, as for example the provision of technical features to present or conceal the caller's telephone number. Those provisions, however, do not relate to the phenomenon normally addressed by the term e-communication. The characteristic feature of e-communication is the technical basis; the existence of a network that is open to all parties connected to it, enabling them to convey signals representing information, as long as some technical standards are being complied with. However, some specific remarks will be made with regard to so called location

[1] Below the question will be discussed whether IP numbers can be regarded as personal data.

based services which may belong to the telecommunication layer, but at the same time raise new threats to privacy.

2 Technical basis of e-communications, TCP/IP-layer, traffic data

TCP/IP is the protocol that is underlying all other services on a higher technical layer on the internet; its technical features are relevant for all other services described in subsequent sections (see figure 2). Consequently, it is necessary to assess the features and possible dangers of this protocol first, analysing in detail what information might be revealed and distributed by means of this protocol, relevant from a data protection perspective.

Application Layer	POP3 (E-Mail), HTTP, SMTP, DNS, ….
Transport Layer	TCP, ….
Network Layer	IP, ….
Link Layer	Ethernet, Wi-Fi, ….

Figure 2: Internet protocol suite

2.1 IP addresses

In order to address any computer taking part in the communication via the internet, an IP number needs to be allocated to it. Under the current protocol conventions, labelled IPv4, IP numbers (also referred to as IP addresses) have the format A.B.C.D, where A, B, C and D are numbers in the range of 0 to 255 (e.g. 195.241.34.113).

In an IP-based network, the set of data that is to be conveyed is being split into small packets of data (not more than 64 KiB), all of which are being sent independently from each other from the sender to the recipient. In order for each packet to find its destination on the way through the net, every packet contains the IP address of the sender and of the recipient. Different from the protocols in use with ‘classic’ telephone communication, no preliminary connection between the devices of the sender and the recipient is being established before conveying the signals. The IP packets will find their way through the net by themselves, being forwarded from one hub or router to the next. The protocol enables the packets to react to any obstacles in their way such as failure or overloading of some routers by changing their route. Therefore it can not be predicted which exact route single packets will take.

Currently, with the older version of the IP standard (IPv4) still prevailing, IP addresses are a limited resource. Even though IPv4 supports up to 4.3 billion single IP addresses, this number is not sufficient in practice to assign a valid address permanently to every user. Therefore, today most IP addresses deployed by private users or smaller companies were assigned to Internet Access Providers who in turn reassign them on a temporary basis to their clients, as

described above. However, it must be mentioned that large organisations and some single individuals also hold a range of IP numbers for permanent use (static IP addresses).

To overcome this shortage, Internet Protocol version 6 (IPv6) has been invented and adopted by the technical regulatory bodies of the internet. The new standard supports 3.4×10^{38} addresses, accordingly every member of the global population of about 6.5 billion people could still use 5×10^{28} such numbers. Its main field of application will be enabling the exchange of data between all kinds of electronic devices. Even though by the end of the year 2005, IPv6 accounted only for a tiny percentage of the live addresses in the publicly-accessible internet, it can be predicted that the relevance of IPv6 will be increasing.[2]

The Domain Name System (DNS; abbreviation also used for Domain Name Server) provides a mechanism for translating domain names into IP numbers. This allows humans to handle easy-to-remember domain names as www.privacyservice.org instead of IP numbers when addressing computers. Such names consist of a top-level domain (the rightmost part; 'org' in the example) and one or more names (two in the sample case: 'www' and 'privacyservice', each separated by a dot. Starting from a domain name, the holder can be looked up in so called Who-is databases, provided publicly by domain name registries (commonly also referred to as Network Information Centre or NIC).

The NIC look-ups enable every interested party to find out to whom the domain name in use with regards to a specific communication is assigned[3]. That way, the main distinguishing element in the TCP/IP protocol, the domain name, as a specific information used for addressing sources of content or indicating e-mail addressees, reveals data of certain persons related to those services.

2.2 Do IP addresses relate to certain individuals?

Moreover, so called reverse DNS look-ups enable users to find the domain name relating to a certain IP number (e.g. 195.47.52.178 to the hostname pc02.uoou.cz). Admittedly, the IP number as it is received e.g. at a web server together with a request for certain information could be entered in such a reverse look-up tool. However, deploying reverse DNS look-ups does not normally lead to revealing users' data. In most cases, the information given will simply refer to the IAP providing the IP number, at worst some details regarding the IPAs staff may be contained (such as contact persons' data). Yet, the IP addresses which are being allocated by the IAP to a user in order to process their requests for information on the internet do not include a hint on the specific users who are sending their requests.

In the current protocol IPv4, IP numbers are a scarce resource. A private person, wanting to access the internet, would generally not be holding a permanent IP number of his or her own.

---

[2] Note that the U.S. Government has specified that the network backbones of all federal agencies must deploy IPv6 by 2008, see http://www.gcn.com/print/25_16/41051-1.html

[3] It is evident that such directories also raise some concerns regarding data protection. Working paper no. 76 of the Art 29 Working Group, issued in June 2003, contains recommendations as to safeguard personal data in this context.

Instead he or she had to rely on the IAP who allocates one IP number out of his contingent for the duration of the internet session (dynamic IP number). It is very likely that with the user's next log-on to the net, he or she will be allocated a different number. The only instance where the allocation of a certain IP number to a user is being stored is the IAP. In these cases, the actual user (the customer of the IAP) can not be traced unless the IAP collaborates (see fig. 3).

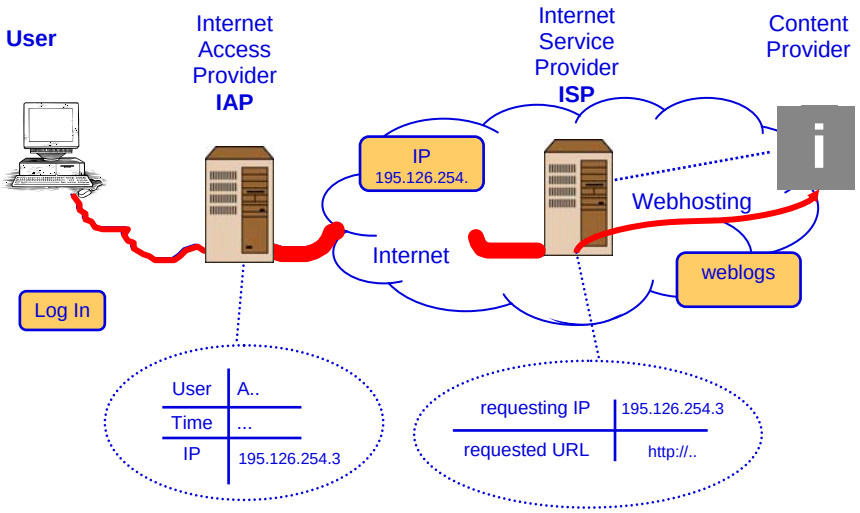


Figure 3: Dynamic allocation of an IP number by the IAP

In other cases the retrieval in a reverse DNS look-up tool may reveal the organisation (such as a company or public sector body as the OPDP in the example given above) the respective IP address was assigned to. Certain larger organisations like companies or public sector bodies may be holding an amount of IP numbers reserved for their own use. Since the legal entity using those IP numbers in the internet is not changing, they are being called static IP numbers. In such cases it is well understood that at least the organisation as such can be recognised from the outside by the IP numbers in use.

Again, contact data of responsible persons at the organisation holding the IP number may be displayed. However, no information on the individual user from within the organisation is being revealed. It has to be borne in mind, though, that likeliness of re-identifying a particular user increases if the organisation abstains from using network address translation (NAT). NAT, regularly installed at the firewall separating the internal network from the internet, is replacing the IP addresses in use in the internal network by other IP numbers when forwarding IP packets to the internet. This technique makes it much more difficult to identify a certain user within in the internal network simply from the IP address that is being deployed when submitting a query to the internet.[4]

The scenarios aforementioned, being the most frequent ones, do not lead to the direct identification of a user. One could find single cases, though, where a domain name is

[4] In this regard NAP may be referred to as a means of achieving more data protection on the internet. With the introduction of IPv06, the need for NAP might disappear, thus creating more privacy concerns.

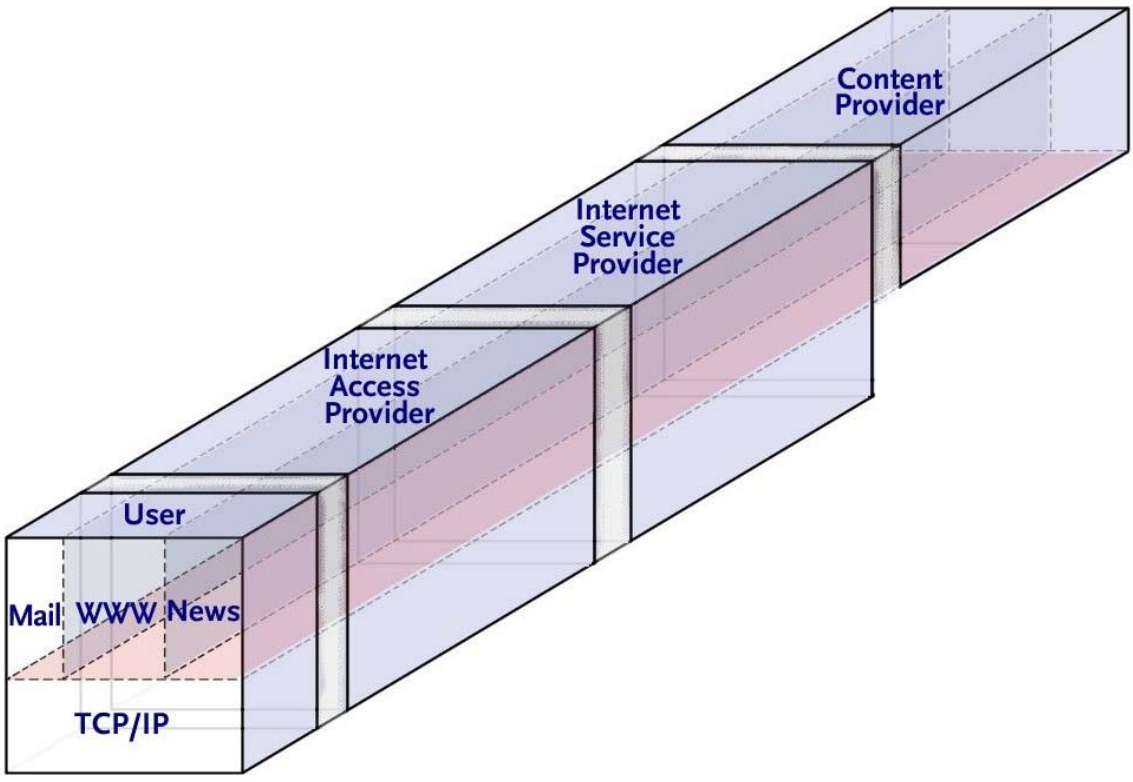
permanently allocated to a single individual, leading to the situation that data deriving from this domain name or the respective IP number might even be personal data.[5]

2.3 TCP protocol

The **Transmission Control Protocol (TCP)** is the intermediate layer between the Internet Protocol below it, and an application above it. TCP enables applications on the network to create connections to one another, over which they can exchange data or packets. In this context, from a data protection perspective, TCP and IP will be assessed jointly. Both protocols form the basis of any application, being handled together by the servers in use with IAPs and ISPs.

2.4 Conclusion

From the technical description given above, a model can be developed in order to depict the deployment of the different technical protocols on different layers and to visualise the involvement of the four prototypical entities. Figure 4 is supposed to explain that the TCP/IP level is relevant in the first place for the user, the IAP and the ISP, whilst the content provider is not necessarily involved into the processing and conveyance of such data which enable the user to communicate on the internet. However, on the application layer, with such protocols as HTTP (WWW), POP3 and SMTP (e-mail), all stakeholders may participate in the communication in a technical sense.



[5] This aspect will be further elaborated in section 3.3.1.

Figure 4: involvement of the four prototypical stakeholders on a technical level

3 TCP/IP layer, traffic data and data protection concerns with regard to the different roles

3.1 User

As it was mentioned above, the user is being allocated an IP number by the IAP in order for him to communicate over the internet. From this it results that the IP number which has temporarily been assigned to a user may be stored at the users communication device. This, however, does not cause data protection concerns. Since the IP number does not reveal any information to the user apart from the fact that it belongs to a range of IP addresses relating to a certain IAP, it is no personal data in the sense of the data protection laws.

3.2 IAP

3.2.1 Storage of traffic data

As described above, the IAP allocates IP numbers to users. In order to enable the technical process of communication on the internet, it is evident that a list of users and allocated IP numbers must be stored as long as the process is still ongoing. From a data protection view, however, the further retention of such lists after the respective communication process is finished becomes problematic. From a mere technical perspective, there is no need to still process such information after the user has logged off or after a certain period of time when the allocation of the previous IP number is suspended.

From a legal perspective, the table (or data base) containing the relation between a user and the IP address, is traffic data relating to a user or subscriber in the sense of Section 90 para 1 of the ECA[6], being 'data processed for the purposes of the transmission of a message via the electronic communications network'. Section 90 para 3 ECA restricts the lawful processing of traffic data to the extent necessary for billing and some other purposes which are not relevant in this context. Section 90 para 2 stipulates the duty to erase traffic data 'once they are no longer needed for message transmission' or the other purposes mentioned in Section 90 para 3 and 4. With a view to data protection controls of IAPs it could be investigated whether they are complying with this obligation.

For the sake of completeness, it should be mentioned that Section 97 para 3 ECA defines a different obligation which may be contradictory, containing a duty to retain certain information. The collision of two conflicting legal duties is solved by the second sentence of Section 90 para 2, according to which the obligation to retain certain data according to Section 97 shall remain unaffected. Section 97 para 3 ECA appears to make use of one possible

[6] This provision correctly transposing Art. 2 b Dir 2002/58/EC.

exemption from the general principle of data minimisation in electronic communication, invoking Art 15 para 1, in particular 2nd sentence of Dir 2002/58/EC. When carrying out data protection controls in this environment, this conflicting provision has to be borne in mind. The exact definition of the extent of such data as well as the time of the storage are being delegated to an implementing legal regulation. As the STE did not hold this provision, no further explanations can be given.

3.2.2 Dir 2006/24/EC - Data retention

In the future, the Section 97 of the ECA must be seen in the context of the new data retention Directive 2006/24/EC. This new provision defines an exact framework of all possible cases of data retention which may be stipulated by national law. Transposing this regulation, member states are not only obliged to introduce a system of data retention if they have not already done so. The Directive also sets limits to the type of date that is to be retained. According to Art 5 of Dir 2006/24/EC, with a view to IAPs, the following traffic data must be retained after transposition of the Directive:

- Data necessary to trace and identify the source of a communication. With a view to IAPs, these are: the user ID(s) allocated, the user ID and telephone number allocated to any communication entering the public telephone network, and the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication (see Art 5 para 1 lit. a subpara 2 of Dir 2006/24/EC).

- Data necessary to identify the date, time and duration of a communication. With a view to IAPs, these are: the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user (see Art 5 para 1 lit. c subpara 2 of Dir 2006/24/EC). Apart from the details mentioned in the bullet point above, the only additional data are the ones concerning time and duration of the communication.

- Data necessary to identify users' communication equipment or what purports to be their equipment. With a view to IAPs, these are: the calling telephone number for dial-up access or the digital subscriber line (DSL) or other end point of the originator of the communication.

It is important, however, to point out that the Directive explicitly abstains from imposing an obligation to collect and retain data which are not already being collected for business purposes by the providers (Art 3 para 1 of Dir 2006/24/EC). As a consequence, IAPs will be obliged to retain at least data on the allocation of IP addresses for certain periods of time to certain users. If they hold additional data of the ones mentioned above, these will have to be retained, too . It will not be required to collect new data only with a view to retention, though.

If, for example, an IAP is offering a dial-in access without prior collection of personal details from the user of a telephone line, such a practice would not have to be changed after transposition of the Directive. The only personal data the IAP had to collect would be the telephone number used when connecting to the dial-in web access.[7]

Further on, it has to be pointed out that Dir 2006/24/EC explicitly prohibits the collection of data revealing the content of a communication (Art 5 para 2). With a view to data protection inspections of IAPs, this could result in the control as to whether URLs visited by the users are being retained. Such a practice had to be considered unlawful, taking into account the principle of confidentiality of communication (Section 89 para 1 ECA). The only lawful storage would be 'the technical storage of data as needed for message transmission' (Section 89 para 1 last sentence ECA). It has to be well understood, though, that the technical process of transmitting a message finishes after the user has received the data, that is when the user's browser has loaded the web page the URL belongs to.

It should also be emphasised that - different from other actors in the field of e-communication, IAPs are not obliged by Directive 2006/24/EC to retain data on the destination of a communication, the reason for this restraint being the fact that by providing access to the internet, IAPs support the deployment of many different services that operate on a higher layer. Therefore, other actors involved might be obliged to reveal such information on the destination of a communication. However, with a view to IAPs, no additional obligations apply insofar.

Directive 2006/24/EC leaves the exact duration of the retention period to the Member States' discretion, defining only a minimum and a maximum period (6 to 24 month).[8] After the transposition of the retention Directive, investigations may be carried out in order to find out whether the time frame as it will be prescribed then by Czech law is adhered to.

3.2.3 Data Security

According to Art 4 of Dir 2002/58/EC respectively Section 98 of the ECA, IAPs are obliged to take appropriate technical and organisational measures to safeguard the security of their services. These measures should be proportional to the risks involved in the specific situation. Additionally they have to inform users about a particular risk of a breach of security. Where the risk lies outside the scope of the measures to be taken by the service providers, they must inform of possible remedies including an indication of the likely costs. Since the enforcement of this provision lies with the Czech Telecommunication Office, the issue will scarcely be relevant during a control.

---

[7] Since the telephone providers will also be obliged to retain data, the allocation of a telephone number to a person could be retrieved, too.

[8] Admittedly, Art. 12 of Dir 2006/24/EC allows Member States to prescribe longer terms than the regular ones defined by the Directive.

3.2.4 Confidentiality

The confidentiality of communications is protected not only by Art 5 of Directive 2002/58/EC but on an international level also by Art 8 of ECHR as interpreted by the European Court of Human Rights. Section 89 para 1 and 2 ECA have transposed the provisions of the Directive. The confidentiality of e-communication, often referred to as the telecommunication secrecy, protects both, content of messages and traffic data including location data. According to these provisions, storage and other kinds of interception or surveillance of communications and the related traffic data are prohibited, except when it takes place in the context of lawful interception of communication by the specially entitled authorities. As far as the storage of messages is necessary on a technical level for the conveyance of a communication in order to deliver the service, it is also exempted from the interdiction. Consequently, sniffing software, monitoring the traffic on a network, looking for certain characteristics (typically the presence of keywords) would be prohibited unless conducted by government agencies, carried out in accordance with the conditions imposed by Article 8 of the European Convention on Human Rights and the national laws.

The distinction between the content of communications and the related traffic data often becomes difficult with a view to certain internet services. For example, the URL a user entered into his browser can be regarded as information on the content even if it is not a descriptive URL. But as Art 5 of Dir 2002/58/EC and Section 89 of the ECA protect both, the distinction is less important in practice. In any event it is prohibited for the IAP to reveal data on the URLs a user has requested or any other information which on the TCP/IP layer is encapsulated within the IP packets and forwarded through the servers of the IAP.

3.2.5 Location data

As mentioned above, this manual concentrates on the core of e-communication. It seems appropriate, however, to give some hints with a view to the processing of location data at this stage. Location data are defined in Section 91 para 1 ECA in compliance with Art 2 lit. c) of Dir 2002/46/EC as data ‘that define the geographical location of the terminal equipment of a user of publicly available electronic communications service’. In particular from the definition given in the Directive (‘indicating the geographical position’) it can be understood that any such information qualifies as location data, however vague it might be. In this sense, an IAP might receive location data by handling incoming phone calls for dial-in connections, displaying the area code. Such data may be processed by the IAP because it forms part of traffic data which is allowed to be processed to the extent necessary for the technical provision of services. Apart from such more unspecific cases of location data, other constellations might occur. Given the fact that the business cases of classic telecommunication companies (telcos) and IAPs mingle more and more, it might be the case that one company which is running a mobile phone network also offers for their clients web access via mobile.

The provider of a cell phone network has the technical possibility to collect location data, to retain and process it; this concerns in the first place the cell in which a user was located when

receiving or starting a mobile phone call. Mobile phone providers will even be obliged to store this information after the transposition of Directive 2006/24/EC (see Art 5 para 1 lit. f). It would not be lawful for a mobile phone providers, however, to disclose such information to the IAP, be it a division of the same company or a different legal entity. Information on the cell in a mobile network from were the communication originated is not necessary for the IAP to technically handle the request to access the internet. Consequently, the IAP is only allowed to process such data if the user has given his prior consent (see Section 91 para 2 of ECA).[9]

3.3 ISPs

Due to the specificities of the TCP/IP standards, at the servers of an ISP in any case the IP address allocated to the user prompting the request will become visible. The ISPs do collect and store such information on a regular basis. The IP addresses are being analysed in order to find out details about the usage of the offers they host. Firstly, in particular with regard to services provided on the word wide web, the way the user clicked himself through the pages is of interest (click stream data). Moreover, at least the country of origin of the request, maybe even a region or a more detailed geographical information can be established. The IP address could also be used to enforce different policies to users from different regions.[10] If the IP address is allocated to an organisation, the latter will be recorded as origin of the request. In the rare case of an IP address statically allocated to an individual having this fact registered in the DNS, such information would also be recorded.

3.3.1 IP addresses at the ISP as personal data?

With a view to investigations and controls, it must be established at first, whether data processing as described above falls within the scope of the relevant data protection provisions. IP numbers and other information kept in a log file at the ISP's servers in the internet are traffic data in the sense of Section 90 para 1 ECA. However, the prohibition to process them and the obligation to immediately delete them does only apply if those traffic data relate to a user or subscriber (Section 90 para 2 sentence 1 ECA, in compliance with Art 6 para 1 of Dir 2002/58/EC). In order to analyse when traffic data relates to a subscriber or user, it is appropriate to get back to a similar term, more popular in data protection: personal data. According to Art 4 lit. a of the PDPA, 'personal data' shall mean any information relating to an identified or identifiable data subject. A data subject shall be considered identified or identifiable if it is possible to identify the data subject directly or indirectly in particular on the basis of a number, code or one or more factors specific to his/her physical, physiological, psychical, economic, cultural or social identity. The criteria for assessing whether an individual is identifiable should also be applied with regard to Section 90 para 2 ECA when gauging the identifiability of a user or subscriber.

---

[9] See below section 8 for more details on location data.

[10] Some e-commerce services reject clients from such countries which are supposed to be the origin of a large number of attempts of abuse and fraud.

It goes without saying that in the case mentioned above[11] where the name of an individual to whom the IP address is being allocated in a static manner can be found simply be means of the publicly available DNS, the IP must be regarded as personal data. However, the situation is not so clear in the two other scenarios mentioned. The decisive question is whether the ISP is able to link the IP number to any other information that reveals the identity of a person.

Before answering the question, it is important to emphasis the purpose and scope of this manual. It is intended to be a guideline to support inspections and controls conducted by the Czech Data Protection Authority. Any official measure taken within the framework of such controls could be challenged in court under the rule of law principle. Therefore, any measure taken should be based on sound interpretation of the law. The argument used in the following passage is striving to provide such 'waterproof' legal basis. It should, however, not be confused with a strategy approach which would be appropriate when a policy paper was prepared.

An ideal-typic ISP is running a server on the internet that is processing requests on the TCP/IP layer in order to provide services on a higher layer. The pure collection of IP numbers that can not be related to a natural person simply by means of DNS or reverse DNS look-up retrieval does not amount to the processing of personal data. On this layer, the provider is lacking means to link the IP address to a person. In doctrine, it is agreed that not just any unlikely possibility of linking a set of data to a person is sufficient.[12] Otherwise, no data what so ever could be excluded from the definition of personal data, since hypothetically it might somehow match a natural person, even though the link existed only for a third party who is not involved and not even aware of the data collection carried out or by deploying a supercomputer which in reality is not available to the party collecting the data. Thus, in order to make the provisions operational, the possibilities of linking must be limited to means which are actually at hand and under control of the party collecting data. Therefore, the use of fictive supercomputers is being left out of account as is any unlawful way to access linking data.

From the ISP's perspective, the only way to create a link from the IP address it collects to identifying information would be approaching the IAP, trying to prompt him to disclose the information. But such disclosure would be unlawful, as can be seen from Art 90 ECA. It would neither be relevant for the provision of the service on a technical level, nor for billing purposes, since on the IP level, most services can be accessed free of charge, and where a fee is being charged this is mostly effected by the service itself on the application layer. As a result, it can be noted that no data on the allocation of IP addresses are allowed to be transferred from the IAP to the ISP.

The result is the same for the second scenario where the IP number is not allocated by an IAP to a customer but by a larger organisation to a member or to an employee. In this case, however, it might be doubtful to apply the ECA. According to German doctrine, a distinction has to be made between two types of communication processes in the context of labour

11 See above section 2.2.

12 Cf. Simitis (ed.), Commentary on the FDPA, 6th Edition 2006, paragraphs no. 30 ff on Art 3.

relations. If the employee is allowed to use the internet (also) for private purposes (e.g. in his lunch break), the ECA and the above subsumption applies; insofar the employer is regarded as having the role of an IAP. When the employee uses the internet for the business purposes of his employer only, the latter is not being regarded as an IAP, the ECA does not apply. Instead, the general provisions of the PDPA have to be complied with. One possible legal basis for disclosure of data from the IAP to the ISP could be Art 5 para 2 lit. e of the PDPA[13]. But the legal requirements of this provision might hardly be met in most cases: The disclosure is neither 'essential for the protection of rights and legitimate interests of the controller' nor the recipient or other third persons. Moreover, such personal data processing would be in most cases 'in contradiction with the right of the data subject to protection of his private and personal life'. Accordingly, also with a view to the second scenario, the ISP had no lawful means to receive personal data from the IAP.[14]

Consequently, it can be noted that the ideal-typic ISP does not process personal data a priory with a view to the first two scenarios. It should be borne in mind, however, that the picture could change taking into account a service on an above layer, carried out by the same provider. If for example the provider was running a shopping system on the HTTP layer, he would normally also collect the name and address when the user places an order. In doing so, he could link this information to the IP address which would become personal data this way. From this moment on, the data protection laws apply. As a consequence, it is prohibited to reveal the path an identifiable user took through different web pages (click stream).

With regard to the third scenario (static IP addresses), however, a legal basis is needed for the lawful processing of personal data. Such a legal basis could be found in the fact that the respective person deliberately effected the entry of his name and the allocated IP numbers in the DNS. In many cases it must be assumed that those individuals, competent in the field of internet technology, had been well aware of the data processing on the net when they decided to appear by personal name in the internet. However, applying the law properly, it would be necessary in the case of any individual's name found on server log files in the internet to assess whether he or she actually gave a valid consent in the sense of the data protection legislation - an undertaking almost impossible to perform.

The result found so far with a view to log files retained by the ISP remains unsatisfactory, since it distinguishes between three scenarios, only two of them outside the scope of the data protection laws and differentiates for the third scenario even according to facts which can not be established in most cases. Consequently, the ISP - possibly by technical assistance - could try to distinguish the log data, only storing the IP numbers relating to scenario one and two and deleting the (few) ones relating to scenario three. He could, of course, also treat all IP numbers as if they were personal data and solve the problem this way.

---

13 Transposing Art. 7 lit. f) of Dir 95/46/EC.

14 It must be admitted that there might be exceptions in special cases, though. Moreover, another legal basis with a view to the disclosure from a public sector employer could be Art. 5 para 2 lit. f) PDPA. This question is outside of the scope of this paper and cannot be analysed more in detail. It should be covered by the second manual that is to be prepared in the framework of the Twinning project.

It is well understood that this question has to be solved before taking on an inspection in this field. Ultimately, it will be necessary to adopt a practical policy with regard to this question. When doing so, the situation as described above should be considered: Any decision could be challenged in court, possibly forcing the data protection authority to change its rulings. From this perspective it could be more advisable only to take actions in cases when undoubtedly infringements were committed.

3.3.2 Dir 2006/24/EC on data retention

It should be mentioned that the new data retention directive does not create any particular obligations for ISPs with a view to retention of log files. Since the Directive strives to harmonise the area and does not leave room for different regulations in the Member States, Section 97 para 3 ECA will have to be amended, also exempting ISPs from the respective provision.[15]

3.3.3 Security and Confidentiality

The obligation to confidentiality and security also applies to the ISP. This leads to interesting results in particular with regard to the telecommunication secrecy. Even if the traffic data and other information collected and retained by the ISP is allowed to be processed because it is not being considered personal data (or relating to a user or subscriber), the general obligation to keep the content of messages and the related traffic data confidential still applies (see Section 89 para 1 of ECA).

With a view to a web server provider, it could be questioned whether any sort of information related to the content is being processed by him at all; even the more so, if all information stored on such servers is publicly accessible. Is there any room for the principle of confidentiality at all? Taking a second look, however, it becomes clearer that in such cases confidentiality does not relate to the content held available on a web server, but to data about access from certain IP addresses to this information. In other words: it is not the content on the web server as such which is protected by the communication secrecy, but the information as to who has downloaded it or read it. It has been mentioned above that the principle of confidentiality is protecting both, content and traffic data, even though it may be difficult sometimes to categorise the data in question. As a consequence, the web server provider has to keep secret the fact that certain (publicly available) content has been requested by and sent to certain IP addresses - even though he is not able to relate those IP addresses to a user or subscriber and thus is not prevented from storing log files containing IP numbers.

As a consequence, it must be considered unlawful if a web server provider publishes detailed log files on the use of his server as it happens in practice in several cases. Such a publication would amount to an infringement of the law. This result is justified, too, considering, that the IAP has different information than the ISP. The IAP, holding a table of allocations of IP

[15] Or rather limiting the obligation to certain types of communications as it is done in the Directive itself.

numbers to users (and being obliged in the near future to do so), would be able to analyse the list published by the ISP and generate personal data out of it, since he would be able to relate it to certain users.

4 Application layer – publishing of content data and data protection concerns with regard to the role of the content provider/ISP

In order to better explain the roles of the content provider and the ISP according to the underlying model and also the dangers resulting from their cooperation, it is more appropriate to slightly deviate from the order used in the section above and to deal next with the content provider. Moreover, as it will be shown below, with a view to content on the internet, it is not useful to distinguish between content providers and ISPs when elaborating further on this issue. This results from two aspects: Firstly, many ISPs do not only offer the possibility to put content created by third parties on the internet but do also provide some content of their own. They practically leave some gaps, some blanks open in their content which others are supposed to fill in. This could also be described as two-stage manner of putting content online. A very popular example can be mentioned to illustrate this phenomenon: A service as *ebay* provides a huge amount of content itself. Nevertheless, this is only designed to be the framework for the content put online by third parties, in this case aiming at providing a platform for auctions. Such services can be regarded as genuine internet services since their business model completely relies on the net, creating a framework of underlying IT architecture and content which others are supposed to use for specific purposes. From this, many practical questions arise, not only with regard to data protection but to matters of liability of the different stakeholders in general.

4.1 Applicable laws

When it comes to the legal assessment of the publication of personal data on the internet, it is most important to ascertain the scope and some established principles of publishing personal data on the WWW. Firstly, the applicable laws must be identified.

With a view to the applicability of different legal regulations on data protection it can be noted that Dir 2002/58/EC does not apply to information society services. According to Art 2 of Dir 2002/58/EC, the general definitions of the so called Framework Directive 2002/21/EC shall apply. Most obligations are aimed at the providers of electronic communications services. According to the definition laid down in Art 2 lit c of Dir 2002/21/EC, the definition of the latter does not include information society services, as defined in Article 1 of Directive 98/34/EC (as amended by Dir 98/48/EC), which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. As it is explained in more detail below in this paper[16], web pages on the internet fulfil the definitional elements of information society services. Since the making available of web pages does not include the

[16] See section 4.5.1

conveyance of signals on electronic communications networks, they are exempted from the scope of Dir 2002/58/EC. Nevertheless, the general data protection directive 95/46/EC does apply.

4.2 The Lindqvist case

The landmark case, decided by the European Court of Justice (ECJ), named after the defendant Bodil Lindqvist has helped to outline some important principles of the application of Dir 95/46/EC.[17] However, some findings of the court remained at least worth a further discussion. Ms. Lindqvist, a Swedish citizen working in a church related community centre, had set up a web site on her personal computer that contained information about her and her colleagues, such as their names, job descriptions, and, in some cases, telephone numbers, family situations and hobbies. It was also mentioned that one of her colleagues had had a foot injury and was working part-time on medical grounds. The publication of these information led to a fine imposed by a Swedish court on Ms. Lindqvist of an amount equal to approximately EUR 450. She was charged of (1) processing personal data by automatic means without notifying the Swedish data protection authority, (2) transferring personal data to third countries without authorisation; and (3) processing sensitive personal data. Ms. Lindqvist appealed the verdict and the Swedish appeal court referred the case to the European Court of Justice for a preliminary ruling.

On 6 Nov. 2003, the ECJ held that

1. The act of referring on an Internet page to various persons and identifying them, directly (name) or indirectly (phone numbers...), amounts to the processing of personal data by automatic means within the meaning of Dir 95/46/EC.

2. Such processing of personal data is not covered by any of the exceptions laid down by the Data Protection Directive (such as processing for purely personal or domestic activities).

3. Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes sensitive personal data within the meaning of Article 8 para 1 of Directive 95/46/EC.

4. Merely making personal data ‘accessible’ on the Internet does not constitute a transfer of personal data to a third country so as to result in application of the Directive's restrictions on international data transfers;

5. The provisions of the Directive do not per se conflict with the principle of freedom of expression or other fundamental rights; it is for the national authorities and courts to ensure a fair balance between the rights and interests in question.

It is most crucial to understand from this ruling that publishing information on the internet can by no means be considered as being a ‘pure personal or household activity’ in the sense of the

[17] Case no. C-101/01

exemption defined in Art 3 para 2 second bullet point of Dir 95/46/EC. The court has emphasised that the fact that data is being published in a media open to worldwide access and technical retrieval where hardly any information ever gets lost or is deleted exceeds the limits of mere personal activities, having potentially enormous effects on the data subject. This decision has had important effects on the work of data protection authorities, obliging them to tackle every complaint dealing with the publication of personal data on the internet.

Some cases that were brought before German data protection authorities show that one of the major problems in this field is the reconciliation between the data subjects interests for data protection and the freedom of speech. The ECJ in its Lindqvist decision has not given much prejudice and left the issue mainly to the discretion of the Authorities and Courts of the Member States.

4.3 Some recent German cases related to published content

4.3.1 Publication of results of sport events on the internet

Some German data protection authorities had to deal with the problem of publicising results of mass sport events on the internet. In principle, two different scenarios can be distinguished, partly depending on the type of sports involved. In most team sports (as football, volleyball), non professional athletes are members of an association or a club. In this case, certain rules can be applied with a view to their membership of the respective body. A working group comprising of representatives of the German data protection authorities responsible for the private sector issued recommendation for such cases. In a second scenario, individual athletes decide to participate in an event without being members of the organising club and without being associated with the organisation a different way (e.g. single persons registering for a city running event). In either case, there is a strong interest of the organisers to publish team lists, lists of results, and rankings on the internet without being obliged to obtain the data subject's consent in every single case.

With regard to the club members, the working group found that firstly it is permissible to publish some basic personal data on individuals having a specific role as representatives of a club or an association. Such data processing may be based on Art 28 para 1 clause 1 no. 2 of the Federal Data Protection Act (FDPA). The latter provision equals Art 7 lit. f) of Directive 95/46/EC.[18] The working group has acknowledged a legitimate interest of the associations as data processors in publishing data of their representatives. As long as only their name, postal address and possibly function within the organisation is concerned, typically no overriding

[18] 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).'

interests of the persons concerned are at stake. Further data as private telephone numbers and e-mail addresses may only be processed after the persons gave their consent.[19]

Secondly, with a view to personal data of active members of such clubs participating in sports events, the working group applied a different provision of the FDPA, Art 28 para 1 clause 1 no. 3.[20] It can not be discussed in detail at this place whether that provision is in compliance with Directive 95/46/EC and if so, which regulation of the latter it transposes. It may be argued, however, that there is some prima facie evidence for the existence of a legitimate interest to process personal data in cases where such data have been published before (Art 7 lit. f). Anyway, the German working group held that the sports events as such were typically public happenings where the interested public had the possibility to learn about details of the persons involved anyway when visiting the event itself. Moreover, in normal cases, there was no legitimate interest of the data subject in the omission of the publication of such data that would clearly outweigh the justified interest of the controller. Therefore, they consider it justified to publish the name, club membership, result and age if necessary of a participating non professional athlete.

However, the working group emphasises that in both scenarios it is crucial to inform the data subject beforehand about the envisaged publication. This would enable him or her to invoke Art 35 para 5 FDPA (which equals to Art 14 lit. a) of Directive 95/46/EC) in the second scenario. The STE does not find this approach particularly convincing, since it amounts to the obligation of a participating athlete to allow his data being published on the internet unless he or she was able to produce 'compelling legitimate grounds relating to his particular situation' (Art 14 lit. a) of the Directive).

According to the opinion of the STE, it would be more convincing if both scenarios were solved in a similar manner, applying the national provisions transposing Art 7 lit. f) Dir 95/46/EC. The common point of both scenarios mentioned is that they deal with members of clubs and associations, in one case representatives, in the second participating athletes. It appears justified to start from the application of the latter provision in such a way that in regular cases, the processing of personal data was justified. But in cases where individual data subjects oppose to their data being published, they should not be referred to the general right to object to certain processing operations since it is difficult to met the prerequisites of that provision. It is more helpful and supporting for the data subjects if their disapproval to their data being published could simply be acknowledged within Art 7 lit. f) of Dir 95/46/EC (or the respective national legislation) as 'reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use'.[21]

---

[19] See annual report on the year 2004 of the Berlin Data Protection Commissioner: http://www.datenschutz-berlin.de/jahresbe/04/teil5.htm#2

[20] It reads as follows: The collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes shall be admissible (…) 3. if the data is generally accessible or the controller of the filing system would be entitled to publish them, unless the data subject's legitimate interest in his data being excluded from processing or use clearly outweighs the justified interest of the controller of the filing system.

[21] Wording of Art. 28 para 1 no. 2 of the FDPA.

The same provision should also be applied with a view to the third scenario where the data subject is not a member of a club but a single individual participating in a mass sports event. The organisers of such events might as well claim that it is in their legitimate interests to publish data on any participant, whereas the persons concerned may as well invoke their prevailing interest of not having their data published that way.

4.3.2 Evaluation of university lecturers on the internet

It was also the Berlin data protection commissioner who had to deal with different web services that offered the possibility for third parties to publish their evaluation on the quality of university lecturers. It is worthwhile noting that different from the first case, the actors involved here are both, providers of internet services, also offering the framework for content to be completed by other users and those very users who would contribute such additional bits of content.[22]

4.3.2.1 Excursus: Liability of the platform provider

It has not been revealed in the annual report of the Berlin Commissioner whether it was also assessed to what extent an ISP as platform provider can be held liable in general for content which is being published by third parties. Art 14 of Dir 2000/31/EC (so called e-commerce directive) is exactly addressing this problem.[23] The provision leads to a situation where the hosting provider is principally exempted from liability unless he has been informed about the illegal information stored on his technical equipment. One could argue, however, that this privilege does only apply in cases where there is a clear distinction between the provider of content and the hosting provider. This might not have been the case with regard to the occurrences the Berlin Commissioner had to decide upon. In that case, the content that was allegedly infringing data protection rights of individuals was created in close cooperation between the provider of the platform and the users who would enter in their appraisals. It was pointed out by the Berlin Commissioner that insofar there is a relevant difference between the creation of a private home page and contributions to an extensive web presentation. Even though in many cases the host providers would also furnish their customers with technical tools enabling them to easily create and publish a home page, host providers have no influence in such cases on the type of content which is being made public by their costumers. This is different with a view to systems as the ones examined by the Berlin Commissioner, where the general structure for the publication had been set up by the service providers beforehand and were the filling in of content created by third users (here: appraisal of university lecturers) is

22 As described above, see introduction to section 4.

23 Art. 14 para 1 reads: Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

the only purpose of the system or where at least the usage of the system for such purposes was known to the owners and apparently encouraged by them. What is decisive, though, is a different aspect. After the platform provider had been informed of the critical legal nature of the content, the obligation was with him to 'expeditiously remove or to disable access' to such information. Accordingly, the exemption from liability had ended after the platform provider had learned about the complaints procedures exercised by the Berlin Commissioner. In such cases, the providers of evaluation platforms can not longer benefit from the exemption in Art 14 of the e-commerce Directive. They can be held fully liable for any infringements effected by means of their system.

4.3.2.2 First case: Unspecific platform used for evaluating university lecturers

In the first case, an existing platform, originally dedicated to give internet users the possibility to publicise test reports of commercial products, had been abused to publish short evaluating texts on university lecturers. These 'test reports' were issued by students, containing their personal opinion on the professor evaluated. This case differs from the one mentioned above, dealing with results of mass sports events insofar as, different from the organisers of sports events, the provider of the platform in which the evaluation was published, had no own interest in the specific content. As regards the evaluating content, the genuine originators were the users who filled in the data base. However, the provider of the platform was held liable by the Berlin Commissioner, since he was the one to maintain the system which was used to publish the data in question.

The Berlin Commissioner held that such a service was infringing the data protection laws and ordered to stop it. In a comprehensive and well-balanced decision the Commissioner weighed the data protection rights against the freedom of speech and came to the conclusion that the first one prevails in this case.[24]

At first it was established that the data concerned was personal data. This was not only true with regard to name, surname and the university related, but also regarding the value judgement itself, delivered by the user. Secondly, the Commissioner stated that the publication of such data on the internet was a way of processing them in the sense of the FDPA. The same result would be found when applying Art 4 lit. e) of the PDPA. Since the professors concerned had not given their consent to the publication, a legal basis for the processing of such personal data could only be found in the law. The Commissioner discussed the application of Art 29 para 1 clause 1 no. 1 FDPA, which is similar to Art 7 lit f) of Dir 95/46/EC and to Art 5 para 2 lit. e) of the PDPA in providing for the balancing of the legitimate interests of the controller against the legitimate interests of the data subjects. This provision was then applied in a twofold way, first with regard to collecting and storing such data on the internet by the service provider, than with a view to transferring those data to third parties, i.e. potentially any internet user.

---

[24] See annual report covering the year 2005, p. 207 ff, download under: http://www.datenschutz-berlin.de/jahresbe/05/bericht_2005.pdf

Since the controller invoked his freedom of expression, this fundamental right had to be taken into account in the reconciliation. However, the protection of privacy prevailed according to the decision of the Berlin Commissioner. Although the Commissioner conceded that in the first place information on the professional sphere of the data subjects was concerned, he nevertheless emphasised that the value judgements on the lecturers were to a great extent based on observations of more personal features and habits which are not part of the professional sphere as such but were taken as an important basis for the subsequent evaluations.

Moreover, the legitimate interests of the data subjects were endangered even the more since there had not been any editorial mechanism to provide for some objectivity. Even though in the general terms of contract, the controller and provider of the service had reserved the right to delete untrue and defamatory statements, the Berlin Commissioner stated that this was not sufficient to prevent from infringements. It could not be proven that the controller had functioning mechanism at hand to recognise and prevent such content. In addition, objective criteria on how to write a 'test report' were lacking. In that, it differs significantly from rankings of universities and professors as they are being published by the media. Such rankings are being based on a scientific approach in order to provide for an objective evaluation, free from unobjective and biased criteria based only on personal motive not related with the original purposes of the evaluation.

Whilst the above aspects already rendered the collection and storage illegitimate, the transfer of those data to third parties, the internet users, was even more problematic. Insofar the provision cited above, Art 29 para 1 and 2 of the FDPA are even more restrictive than the Directive. Whilst for the application Art 7 lit f) of Dir 95/46/EC it is sufficient that the controller as the party who is transferring the data has a legitimate interest, Art 29 para 2 no. 1 requires a legitimate interest of the recipient. This is something which can not easily be verified unless the parties accessing this data base through the internet had to log-in individually in order to retrieve the data base.

4.3.2.3 Second case: specific platform 'www.meinprof.de'

Very recently, the Berlin Commissioner had to deal a second time with a similar problem.[25] The difference with the new case was that a web platform had been specifically launched for the purpose of offering a tool for students to publish their (anonymised) appraisal of the professors. Different from the first case, no doubt could occur as to whether the provider of the web site could be held liable for the content. Although the appraisal as such was delivered by third parties, the web site provider must be held completely liable for the content. He did not only create the web front end but has explicitly dedicated it to the purpose described above. Moreover, he has provided a system were users are supposed to enter in certain criteria, categorised by the ISP. Basically, all marks given by the users (students) are being aggregated to a value equal to a school mark. This also serves to generate so called lists of tops and flops,

[25] See http://www.heise.de/newsticker/meldung/76754

displaying the lecturers with the best and the ones with the worst marks. However, the input of certain individuals remains visible in a table where the single marks given by each user plus a remark in free text are depicted for every course that is being evaluated.

Apparently, there are two types of users, registered and not registered ones, which means that anybody can submit their evaluation without checking in any way who they are. As a comfort for the lecturers under scrutiny, a particular section of the web site is informing them on the functioning of the service. During the preparation of this report, the service provider has apparently reacted to the criticism and announced that he plans to implement a feature securing that only such individuals would be allowed to fill in their evaluation who were actual participants of the courses under evaluation. In addition, users should be prevented from entering more than one entry for one course they attended. Further plans involve the issuing of one-off passwords to be distributed by the lecturers to the students. Such amendments to the service would help to overcome doubts as regards the lawfulness. If a lecturer was requesting such a list of passwords from the service and distributed it to the students, such an act would have to interpreted in such way as to the lecturer giving his consent to the publication on the web.

According to the standards defined with the first case, the Berlin Commissioner has advised the ISP/platform provider to change certain functions of the service. Most important, he insists on informing the data subjects prior to the publishing of any evaluation about them. Moreover, the Berlin Commissioner has demanded that the page should only be accessible for such users who would first register themselves with the service. This is supposed to prevent from unauthorised download. When registering, users could be asked for the reasons why the information was needed, thus proving their legitimate interest to access those data. The problem mentioned above with a view to Art 29 of the FDPA could be overcome this way. The service could accordingly be provided in a lawful manner if two requisites were met: Access only to a limited number of persons who have to be pre-registered and in addition, proper information of the data subjects. The data processing would be based on Art 28 para 2 no 2 FDPA (transposing Art 7 lit. f) of Dir 95/46/EC). If after proper information the data subject objected to the publication, he or she was supposed to have claimed that their legitimate interests prevailed in the sense as stipulated by the provision cited above.

However, if the business case was changed slightly and entirely based on the cooperation of the lecturers in the way described above, the consent of the person concerned would exist. With a valid consent in unrestricted publication, the limitation of access only to such users which have registered beforehand would not be necessary.

4.4 Generalisation: Application of the basic principles of Dir 95/46/EC

From the cases explained above, some general findings can be extracted and applied to the controls and investigations in this field. First of all, the publishing of personal data on the internet has to be in compliance with the relevant provisions of Dir 95/46/EC respectively the national legislation transposing those regulations.

4.4.1 Data must be processed fairly and lawfully

Firstly, Art 6 of Dir 95/46/EC must be adhered to, obliging the data controller to provide for compliance with the fair and lawful data processing principles. It is at least questionable if the publication on the internet can still be assumed to be fair and lawful in cases as the ones elaborated on above, where a third party would enter in personal information, possibly without the data subject even knowing about it. As far as the freedom of expression is concerned, reconciliation has to take place to balance the fundamental rights involved. It should be taken into account in this context, however, that Art 9 of Dir 95/46/EC points into a certain direction: At least the processing of personal data for journalistic purposes or the purpose of artistic or literary expression is being privileged and exempted from the scope of the Directive. It could be questioned as to whether other types of publications which do not meet the standards of journalistic work should be exempted, too. On the basis of these considerations, it appears to be unfair to process any information on a third person, be it even on somebody in a prominent position as the one of a university lecturer.

4.4.2 Limitation of processing to predefined purposes

When processing personal data, the principle of limitation of purposes is one of the crucial aspects. When adhered to, it is a very effective safeguard to realise the fundamental right to informational self-determination (as the German Constitutional Court put it[26]), allowing the individual not only to keep track of his data but also to effectively restrict the ways they are being processed.

It becomes clear from the description of some practical cases given above, that for data published on the internet, limitation of purposes is but a fiction. Even though the terms of use of some web sites may stipulate the obligation to use personal data only in a certain way, it is almost impossible to enforce such restrictions unless official public procedures are concerned.[27] It goes without saying, on the other hand, that in the private sector, no effective remedies are at hand to come to a similar effect.

From this it becomes apparent that the best way to provide for lawful processing of personal data by publishing it on the internet is to base the processing merely on the consent of the data subject. If an individual, duly informed on the effects of publishing his or her data on the internet, still agrees to give consent, no doubts as to the legal basis can occur. In the case of so called sensitive data (Art 8 of Dir 95/46/EC) specified consent is needed, relating expressly to those data.

---

[26] BVerfGE 65, 1 (official collection of the cases decided by the German Federal Constitutional Court, volume 65, page 1)

[27] If, for example, some data may not be used against the data subject, he or she might invoke this clause in a court procedure, thus effecting a ban on using such information.

4.4.3 Further principles which must be complied with

The further principles (Art 6 lit c) to e))must also be complied with, providing for limitation of processing to the data actually necessary (also called principle of data minimisation) and for accuracy of data, including the obligation to rectify data where necessary. Another aspect of data minimisation is to delete data or at least the elements relating to a natural person as soon as possible.

4.4.4 Deletion on the internet and search engine caches

It should be mentioned that in particular the timely and complete deletion of inaccurate data turned out to be a problem with a view mainly to search engines. These services do not only on request provide a list of URL where the terms searched for can be found. Moreover, they tend to cache the web sites their computers have indexed, leading to the situation where even after deletion of the original unlawful publication some remainders will be found on the net.

Amongst the data protection authorities in Germany, the question was discussed who can be held liable for such caching by search engines. The one who is to be held liable in the first place is the originator of the incriminated content. This original content provider may take some technical measures in order to prompt the search engine mechanisms to update their caches: All so called web crawlers deployed by search engine providers are programmed to first read the file 'robots.txt' in the root directory of a domain. This file can be used to advise the crawlers to skip certain areas of the web site. In the above case, the web page where deletions were effected, could be indicated as not allowed to be indexed by search engines. This should lead to the extinction of such entries in search engines.

Another option would be to hold the respective search engines themselves liable. A German court decision had pointed into this direction. The court had held that even the provider of a so called meta search engine may be held liable. Meta search engines are not deploying web crawlers of their own but are merely summarising and displaying the results of queries to a number of other regular search engines. According to that court ruling, a provider of a meta search engine shall be obliged to bar such links that lead to unlawful content (offensive publications in this case).[28] Although this verdict has been quashed subsequently by the appellate court taking into account the specific facts of the case[29], both courts left no doubt that at lease the provider of a simple or regular search engine bears the legal duty to prevent by technical measures access to web sites which contain unlawful information if the search engine providers are requested to do so. The general principles of liability are relevant for such cases, since in compliance with the e-commerce Directive, Art 21 para 2[30], no specific exemptions for providers of search services can be applied. It should be noted, though, that in this case the search engine provider of 'Yahoo!' had immediately after notifying about the illegitimate content taken measures to prevent users from finding the disapproved content by

28 Landgericht Berlin, decision of 22/02/2005, 27 O 45/05.
29 Oberlandesgericht Berlin, decision of 10/02/2006, 9 U 55/05
30 See above on liability in general, section 4.3.2.1.

adding the critical search term to a blocking list. On the other hand, data protection authorities in Germany found it difficult to get into contact with the operators of the Google search engine, based in the USA, in a similar case. At the time of the preparation of this report, the discussion in Germany is still ongoing.

4.4.5 Lawful processing criteria

In addition to the fair and lawful processing principles, the criteria of Dir 95/46/EC as transposed by the national legislation must be complied with when publishing personal data on the internet.

As mentioned above, the most reliable way to come to legitimate data processing is to obtain the consent of the data subject (Art 7 lit a) of Dir 95/46/EC). From the other possible grounds for lawful data processing, only lit f) may be of a certain relevance.[31] Nevertheless, the analysis of the cases mentioned above leads to the result that only in specific situations the publication of personal data on the internet may be justified by this provision. Admittedly, the necessity of the data processing 'for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed' can be assumed in many cases, given the fact that such legitimate interest does not require a specific legal relationship between the controller and the data subject but merely an economic interest in compliance with the law. However, on the other hand, the 'interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)' are likely to override the position of the controller in most cases. This is mainly because of two aspects: Firstly, the data published on the internet can be accessed by everybody worldwide and for an immense time span. Deletion mechanisms are not effective unless they are positively taken care of. Secondly, all information on the web can be retrieved easily and combined with other information available to a profile of the person concerned. All this leads to the assumption that in most cases the interest of the data subject to be protected against the consequences of such processing operations prevail. Sometimes, against such a balancing of interest in the favour of the data subject, the argument is brought forward that the data subject in most cases would not even care about the publication. This is not convincing, however. If that assumption was really correct, it would be no obstacle to obtain a valid consent form the data subject. As a consequence, only in exceptional cases the provision cited above may be applied, e.g. when there is a specific relationship between the controller and the data subject and only a set of basic data is concerned.[32]

---

[31] It should be noted, however, that particular provisions might apply to public sector bodies, possibly based on Art 7 lit e).

[32] In the opinion of the STE it is more than doubtful whether such criteria apply the cases mentioned above related to results of mass sport events. From the majority that might not bother, consent can be obtained. For the rest there should be no insinuation that they would not object. It must be taken into account that the internet may serve as a source of information for anybody for all purposes. Would a participant want a possible future employer to know that he tried to participate in the local 10 km run but did not finish?

There are more specific regulations to be found in Art 8 of Dir 95/46/EC that may serve as basis for the processing of special categories of data in the sense of the directive. However, in particular with a view to those sensitive data which are subject to even more restricted provisions, it is difficult to imagine any other legal basis for the publication of such data on the web except for the informed and specific consent of the data subject.

As it was set out above when reporting on the Lindqvist case, the ECJ is of the opinion that the publication of personal data on the internet does not amount to a transfer of such data to third countries in the sense of Art 25 ff of Dir 95/46/EC. This part of the decision was criticised sharply and simply does not fit with the legal system of the Directive. If the Lindqvist decision was applied, the publication of data would not have to be measured against the relevant provisions of the Directive. However, if the data subjects consent was obtained prior to the publication, also Art 26 para 1 lit a) of Dir 95/46/EC can be applied, thus even justifying the transborder data flow. In order to produce a valid statement of informed consent, it appears sufficient to simply inform about and let the data subject sign that the data is going to be published on the internet. It is common place and known to every body today that this implies the worldwide accessibility and possibility to retrieve such information.

4.5 Problems in enforcement

During the discussions held with representatives of the OPDP, cases were reported in which the investigation of complaints was hindered by practical problems. Such problems are not unknown to German data protection authorities either.

4.5.1 Excursus: Scope of the obligation to inform about personal details of the originator of content on the internet

One practical problem might be to find out the natural or legal person responsible for certain content on the web. In this context, Dir 2000/31/EC (e-commerce directive) must be taken into account. According to Art 5, all service providers shall be obliged to provide certain information to their recipients, including the name of the service provider, the geographic address at which the service provider is established (note: a post box address would not be sufficient), further details including his electronic mail address. If this provision was adhered to, it should not be difficult to identify the natural or legal person responsible for certain content on the internet, provided that the obligation was intended to address every single provider of content, be it even a small private home page.

The obligation is addressed to service providers. According to Art 2 lit b) of the e-commerce directive, a service provider is any natural or legal person providing an information society service. For the definition of the latter term, the e-commerce directive refers to a different legislation: Art 1 para 2 of Dir 98/34/EC as amended by Dir 98/48/EC. According to the regulation effected by the amendment, this provision does not exactly define the term information society service, but the more general term ‘service’ is being defined as ‘any Information Society service, that is to say, any service normally provided for remuneration, at

a distance, by electronic means and at the individual request of a recipient of services'. Further parts of the provision try to bring more clarity to this partly obscure definition, an annex to the regulations aims to name some services which were not intended to be within the scope of the definition.

When the e-commerce directive was transposed into German national law, there was a debate going on as to whether the obligation to give name and address details had to be applied to mere private, non commercial web sites as well. As a result, it was found that also private content providers would fall within the scope[33] and the following arguments were brought forward: Without any doubt, a private home page is to be considered as a service provided 'at a distance', meaning that the service is provided without the parties being simultaneously present (see Art 1 para 2 of Dir 98/34/EC as amended by Art 98/48/EC). It goes without saying that the service is being provided by electronic means in the sense of the latter provision. Moreover, the service is being provided 'at the individual request of a recipient of services'. According to the provision cited above, this 'means that the service is provided through the transmission of data on individual request' - an explanation which is not particularly helpful. However, the annex mentioned above gives a hint as to what was intended to fall within the scope of the definition by naming some examples for services that should not be covered. In annex V under no. 3 it reads: 3. 'Services not supplied "at the individual request of a recipient of services" (are) Services provided by transmitting data without individual demand for simultaneous reception by an unlimited number of individual receivers (point to multipoint transmission)', in addition giving some examples, such as TV and radio broadcasting services and teletext. Different from the services mentioned, all information distributed via HTTP and similar protocols based on the TCP/IP layer have to be requested by a user in order for him to receive it. Different from radio and TV, there is no broadcasting of such information. In the case of broadcasting, a recipient just has to switch on his receiving device and will thus receive the signal without further prompting it. On the internet, in contrast, in a technical sense the recipient has to prompt all information flows in a technical sense. Therefore, also the last definitional element of the above provision is met.

Nevertheless it could still be argued, that it is doubtful whether a private home page can be regarded as a 'service normally provided for remuneration' in the sense of the provision above. Most home pages, not only private but also commercial ones, are in fact being provided without charging the user to see (or receive) it. The definition leaves open a loophole, however, since it does not demand that remuneration is the case with every web page, but just 'normally', thus allowing for exceptions. At this point, two arguments can be brought forward as to why home pages in general fall within the definition of Information Society services. Firstly, the definitional elements apply to commercial and private web sites in the same manner, including the possible objection with regard to the non existence of remuneration for receiving the content of the web site. Yet, at least with regard to commercial web sites, the obligation to inform on certain basic data in accordance with Art 5 of the e-commerce directive seems to be common sense. It would be logically incoherent to base the alleged

[33] See Art 6 in connection with Art 3 no. 1 Tele Services Act (Teledienstegesetz of 1 August 1997, last amended 14 December 2001); http://bundesrecht.juris.de/tdg/index.html

exemption of mere private web sites solely on the absence of remuneration, since the latter is a common feature of both, private and commercial web sites on the internet: the basic service, the possibility to receive information, is offered for free, this is not the exception but the rule in either case.

Secondly, the additional and more specific obligations to inform according to Art 6 of the e-commerce directive must be taken into account. Such further obligations are limited to 'commercial communications which are part of, or constitute, an information society service'. If a commercial web site was not regarded as an information society service, the provision could not be applied to it. As a consequence, all specific information required by Art 6 could be missing on a web site even if it was undoubtedly a commercial one - a situation which would not be in compliance with the transparency requirements as described by the legislator of the e-commerce directive in recital 29.[34]

4.5.2 Possible actions against the ISPs

Even though the law imposes the strict obligation to indicate a person responsible for the content published on the web, this regulation is not always adhered to. According to the principles explained above on the liability of the host provider[35], the latter should be addressed in such cases. By looking up the domain name (which is the minimum information that will always be available) in a Who-is data base, the ISP hosting the content can be found. Most ISPs are cooperative when approached by a public authority; for the rest their legal obligations have to be clearly set out. If the compulsory imprint of a web page is lacking, the content is not in compliance with the law and must be taken off the internet. Exercising the powers of a control authority, the ISPs could be requested to present all documentary they have retained related to the respective costumer. This information could directly lead to the identification of the responsible person sought for or (as e.g. an e-mail address) serve as starting point for further investigations.

4.5.3 Cases involving providers based outside the national territory

If the web server is located outside of the respective country, further steps depend on the actual situation. Firstly, the physical location of the server does not necessarily have to be decisive when ascertaining the remit of the respective authority. What is relevant is whether

[34] In cannot be ruled out, however, that this was the understanding the Czech legislator had when transposing the e-commerce directive. This was being effected by enacting the 'act on certain information society services and on the amendment to certain other acts (Certain Information Society Services Act)' which did not impose a comparable obligation to information on providers of web pages. It cannot be ascertained by the STE whether the newly introduced paragraph 4 of Section 53 of the Czech Civil Code is sufficient; in order to understand this part, it would have been necessary to analyse the addressees of the previous provisions. However, from the localisation in the Civil Code it is likely that it applies only the contractual relations and to relations prior to entering into a contract. A user simply visiting any web site is not in this position. At least in the understanding of the German legislator, the provision of the e-commerce directive has a more general scope, creating an objective obligation for all web page providers independent of possible contractual relationships.

[35] See above 4.3.2.1.

the ISP as a legal or natural person falls within the remit of the respective authority. The ISP is the one technically responsible for the web hosting. In many cases, such companies cooperate with subcontractors who could as well be located in a third country to provide their services. If the ISP is located in another EU Member State, the respective national authorities in that state should be approached. Given the cooperation on the European level in Art 29 group and other parties, a common understanding of the issue should be reached. If the ISP was located in a third country, it could be useful to try to address him more informally. However, it is well understood that in those cases the limits of enforcement capabilities of national data protection authorities in the EU may easily be reached.

5 Application layer – dissemination of content - Unsolicited marketing communications – Spam protection

5.1 Relevant provisions of Dir 2002/58/EC

One of the most urgent issues in the internet are unsolicited marketing communications, usually carried out by e-mail, often referred to as 'spam'. Directive 2002/58/EC contains at least two regulations which are important for this sector.

Directories of e-mail addresses are governed by Art 12 which prescribes basically that subscribers must be informed, in advance and free of charge, about the purpose of a public electronic directory. Moreover, they must be given the opportunity to determine whether and to which extent their personal data are included in a public directory. From this it results that it is unlawful to create an e-mail directory without at least giving the individual subscriber the opportunity to object (opt-out system).

Moreover, in Art 13 of Dir 2002/58/EC, four basic rules regarding the lawfulness of sending unsolicited communications are spelled out.

- Automated direct marketing is prohibited in principle:

  The use of automated calling machines, fax or e-mail for the purpose of direct marketing is only allowed with the prior consent of the subscriber (opt-in system) (Art 13 para 1).

- Privileged: marketing communication within existing business relationship:

  Only in cases where a person or a company had obtained the e-mail address in the context of the sale of a product or service, this person or company may use the e-mail address for direct marketing of its similar products or services. In such cases, customers must clearly and distinctly be given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially

refused such use. This results in a privilege for legal entities having previously established a business relationship. However, the recipient has still the right to opt out at any time. In order to facilitate the exercise of this right, the sender is obliged to inform of ways of opting-out (Art 13 para 2).

- With regard to means of contact other than automated ones, and in particular to individual marketing phone calls, Member states are free to establish either an opt-in or an opt-out system (Art 13 para 3).

- In any event, it is illegal to disguise or conceal the identity of the sender on whose behalf the direct marketing communication was sent. From this an obligation to inform properly on the identity of the sender emerges. In addition, a valid return e-mail address must be provided to which the recipient may send a request that such communications cease (Art 13 para 4).

In Germany, the data protection authorities received many complaints regarding unsolicited e-mails. These complaints could not always be pursued. Different from the Czech Republic, where according to section 10 para 1 lit a) CISSA, the Personal Data Protection Office is in charge to carry out the supervision of compliance with regard to dissemination of commercial communications, in Germany there is missing a special provision authorising the data protection authorities in this field. Ways were found, however, to tackle at least those cases which could be addressed within the remit of a classic data protection authority.

For this purpose, general data protection provisions were applied, mainly the national regulation equalling Art 7 lit f) of Dir 95/46/EC[36]. From this provision it derives that collecting of personal data like e-mail addresses for the purpose of unspecific future communications (marketing) on the Internet is unlawful. The act of using such data for the purpose of marketing cannot be deemed to be 'necessary for the purposes of the legitimate interests pursued by the controller or by the third party'. This derives from the fact that any unsolicited marketing communication via e-mail is prohibited unless the addressee gave his previous consent or business relations were established earlier. Where neither is the case, a person must not be addressed by e-mail. Applying the principle of data minimisation and the not excessiveness of data at the same time, it becomes clear that there is no legal ground available for the storage of lists of e-mail addresses. On this basis, data protection authorities in Germany demanded of previous 'spammers' to delete lists of e-mail addresses found with them.

At this point an outlook may be given: it is expected that as a consequence of the fast dissemination of telephone serviced based on the voice over IP protocol (VoIP), spamming will also decrease with regard to telephone calls. Even thought the regulations of Dir 2002/58/EC strictly prohibit automated marketing calls, such molesting calls might still occur more frequently, triggered from third countries where the regulations cannot be enforced. The

[36] Which is Art 28 para 1 no 2 FDPA, as cited above in footnote 20.

ICPP in Kiel is involved in a European project aimed at introducing counter measures to prevent from such future threats.

5.2 Verification of consent to the reception of e-mail messages, double opt in

In the context of unsolicited e-mail communications, it is crucial for such service providers who are striving to offer lawful services that they are able to obtain a consent from the users in a manner that is both, legally valid and practically feasible. This is of particular importance for such services whose major activities consist of sending e-mails on a regular basis e.g. to inform the recipient of ongoing developments in any sphere or to promote current special offers. These services are often referred to as newsletters. According to Art 2 lit h) of Dir 95/46/EC, 'the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. Moreover, in Art 7 lit a) it is set forth that the data subjects consent must be given unambiguously in order to form a legally valid basis for data processing. As it will be explained in greater detail below, the German laws entail a more detailed regulation as to how consent can be obtained on the internet.[37]

In order to meet the legal requirements and to undoubtedly receive a valid consent form the users, the following procedure had evolved for newsletter providers in Germany: In a first step, the user is asked to enter in his e-mail address in a web form and to press an additional button to submit it. In a second step, a confirmation e-mail is sent to the respective e-mail address which was entered in. With this e-mail, the recipient is requested asked to confirm that he actually has ordered the service. To this end, the recipient is requested to send back an e-mail reply by just clicking the reply button in his mail client. Only after the provider has received this confirmation, the recipients address is permanently added to the lists of subscribers. This procedure secures that the newsletter is only send to persons who have unambiguously given their consent.

Even though the procedure was approved by courts and the data protection authorities, one recent court ruling found that is was not sufficient.[38] The plaintiff criticised that he had received the request for confirmation by mail even though he had never put in his address on the web site of the provider and had never requested those services. In fact, following the procedure described above, it is inevitable that the request for confirmation is being sent to any address which was entered into the web site. If a third person has entered in the address of somebody else, it is also inevitable that this addressee will receive a request for confirmation which he has not prompted himself. However, the request for confirmation is the only annoyance the addressee has to bear; if he simply does not respond, no further mails will be sent to him. Nevertheless, applying the law verbatim and in a strict manner, the judge found that it was even an infringement of Art 13 para 1 of Dir 2002/58/EC (respectively the national law transposing the regulation) because the prior consent required by the latter provision was missing. It remains to be seen, however, if higher courts will follow the referred decision. To

[37] For more details, see section 6.3.2.3.

[38] LG Berlin 16 O 268/06, Judgement as of 29/08/2006, not yet published.

apply the laws in such a strict manner might impede the development of online based services considerably, because it can not be seen how a legally valid consent can be obtained unless resorting to paper procedures, apparently a very poor option.

6 Application layer – online collection of content - data protection concerns with regard to the different roles

6.1 User

With a view to data collection and further processing by the user, general principles apply. Firstly, it should be pointed out that the user's data processing activities fall outside the scope of the ECA respectively Dir 2002/58/EC. Instead, general regulations apply, in particular the PDPA. Controls or investigations of users, conducted by the data protection authority, could only take place if data processing is not being carried out by a 'natural person for personal needs exclusively' (see Art 3 para 3 PDPA, in compliance with Art 3 para 2 second bullet point of Dir 95/46/EC). Whilst this provision exempts any private activity by single users from the application of the PDPA and thus from investigations and controls, the most relevant cases where infringements may occur are data processing of larger organisations, be it of private or public nature.

Such organisations may be interested in personal data from the WWW for a variety of reasons. For the purposes of this report, certain activities of State bodies that pursue specific aims and are governed by special legal regulations may remain outside the scope; a typical example being criminal prosecution according to the criminal procedure code. Other public or private sector institutions could be interested in collecting personal information on the internet for other more general purposes, as for example the appraisal of an application for a job. It can be assumed that many HR divisions are conducting a web research in order to find data on a candidate. The aim can be to find additional information or to verify statements made by the person concerned.

Such collection of personal data on the internet is in compliance with the data protection laws as long as it is confined to such data which the data subject has made public himself. Because of the generally insecure environment of today's WWW, in many cases there will be no ultimate proof of authenticity, that is as to whether some information actually derives from the data subject. Nevertheless, it should at least be paid regard to some important indicators. If a complete private website of a person exists, it is rather likely that he or she has published it him- or herself. The same is true for personal information published in certain services (such as openBC) which apply some routine checks to make sure that only the data subjects publish and edit their data. From a legal perspective, collecting such data can be based on the consent of the data subject. Even though some formal aspects of a valid consent are missing, it must be presumed that a person publishing his or her data in a medium like the WWW accepts that they can be used by everybody for any purposes in compliance with the laws.

Interestingly enough, this legal principle is also reflected in Art 8 of Dir 95/46/EC, dealing with so called sensitive data. Even for those special categories of data, processing is permitted if it 'relates to data which are manifestly made public by the data subject' (Art 8 para 2 lit. e).

The fact of voluntary publication by the data subject might be less evident with respect to other types of web pages which contain information on several individuals in a certain context. One example is the home page of an institution, publicising information about its employees. Although in Germany it is highly recommended to do so only with the data subjects' consent, one should be aware of the fact that this is not always complied to. Data protection authorities were also dealing with other examples, related to sports events (as a city marathon). It turned out that in some cases, the organisers had linked their registration software and their system of time measurement (which is done automatically by RFID tags to be attached to one's trainers) with the web page of the event in such a manner that all participants would automatically appear on the web page with their names and the results. It goes without saying that such a combination is unlawful, preventing the data subject from actually exercising his right to freely decide whether he gives his consent to the publication.[39] If such data were collected by a user for other than purely personal or household activities, the collection of the published data might easily turn out illegitimate, since they had not been made public on the initiative or with the consent of the data subject.

This may be even more obvious with other examples where the missing consent is almost palpable. This is the case when the name of a person appears on so called revenge pages which are designed to undermine the reputation of persons. Data from such or similar pages should never be collected when doing research on certain persons on the internet since their processing by the collecting party is unlawful a priori.

Another aspect should be borne in mind when it comes to personal data collection on the internet. Apart from a few exotic cases it is rather difficult to decide if data found when searching for names is actually relating to the targeted person or to a namesake. If the latter is the case, the data collected and stored is being incorrect, thus creating the obligation to correct it, that is delete the part referring to a different person.

All this leads to the conclusion that collecting personal data on the internet is not prohibited per se. But an organisation doing so must be well aware of the dangers and legal limitations. From the perspective of a data protection authority, these aspects could be addressed in a control. Generally, the onus is on the data controller to prove that personal data processed has been collected in a fair and lawful manner (see Art 5 para 1 lit. c PDPA and Art 6 para 1 lit. a of Dir 2002/58/EC). If this can not be proven because some sources appear doubtful or cannot be reconstructed at all, the respective data has to be deleted.

Moreover, one specific case of collection of personal data from the WWW may take place in relation to the use of e-mail addresses for marketing purposes. Since the sending of commercial communications by e-mail is only allowed if the user gave his prior consent or it

[39] For a more detailed assessment see above, section 4.3.1.

happened in the context of existing contractual relations (see Section 7 of the CISSA and Art 13 of Dir 2002/58/EC), it can be ruled out that the collection of e-mail addresses is pursuing a legitimate purpose.[40] Accordingly, any such collection and storing is to be considered unlawful, the e-mail addresses gathered that way must be deleted.[41]

6.2 IAP

It has already been mentioned above that the IAP is not permitted to store any data on the content of e-communications conveyed over the internet.

6.3 Content provider/ISP

Apart from the publishing of content on the web, the other most relevant situation when it comes to the processing of personal data is the data collection in the context of the provision of services on the internet. The general data protection directive 95/46/EC does also apply to these constellations.

6.3.1 Cases the German data protection authorities or courts were concerned with.

6.3.1.1 Excessive collection of information in the context of ordering goods or services through the internet

German data protection authorities have received complaints regarding the collection of personal data of users when they were performing on-line shopping or were contracting with similar services. Normally, in such cases only a basic set of data is necessary for the performance of a contract, consisting of:

- name of the contracting parties,
- modes of payment and related information,
- postal address in case some good has to be delivered to the costumer.

In cases where the purchased item is comprised only of electronic data, strictly speaking not even an address information would be necessary if the product can be downloaded directly from the web page. However, other business cases might involve providing the costumer with a log-in for the download which he only receives after the verification of the payment. In such cases it may also be justified to require the e-mail address.

---

[40] See above, section 5, were the issue is elaborated upon more in detail

[41] This is true at least for entities intending to use them for commercial mails. Depending on the legal situation in the Czech Republic, different results might occur with a view to entities active in the field of political campaigning.

In practice, however, many online shops and services tend to require excessive data or do even force the customer to establish a user account with the respective supplier, retaining the data for a time span longer than it is actually necessary to completely carry out the individual order.

The data protection authorities were stressing that any data collection and processing that is not strictly necessary with a view to the performance of the contract may only be executed on the basis of a valid consent.

In other cases, users had complained that they were not allowed to participate in a public forum on the internet without leaving certain details. The providers of such forums would only allow them to contribute to the content after registering, indicating certain particulars.

Such a practice can also be noted with other services. In Schleswig-Holstein, a public swimming pool presented its premises and special offers on a web page. Users could even subscribe to a newsletter of the institution. It is evident that the only data strictly necessary in order to deliver such a service, is the users' e-mail address. However, it turned out that some more data was requested, including the user's name. The data protection authority pointed out that any additional data in excess of the e-mail address could not regarded to be lawful with a view to the transposition of the criteria for lawful processing into German law. The service then abstained from the previous practice, indicating that any additional input of data was only voluntary, but might serve the convenience of the customer (e.g. to be addressed in a politer way by ones name).

One key argument in this dispute was that non of the additional data sought by the provider could verified, thus not being reliable anyway. In such circumstances, strictly applying the principle of necessity, any data exceeding the absolute minimum could only be collected on a voluntary basis. Admittedly, under certain circumstances and for particular services[42], additional data may actually be needed. But invoking such a need and at the same time abstaining from implementing means of verification of the data amounts to a contradictory and thus invalid argument. Declaring those additional fields to be voluntary, on the other hand, does only sanction the existing situation and makes it more transparent since de facto the entering in of real and accurate data can not be enforced by any means. This fact should be announced openly, making it transparent to all users.

A similar case was encountered in a different Member State, the Republic of Malta, when using a wireless internet hot spot in a hotel. The provider offering the service also prompted its users to enter in their name when all that was needed were some numbers distributed by means of a prepaid voucher that had to be acquired prior to the use of such services. The Maltese data protection authority had assessed the issue and came to the same result, pointing out that the additional data was not necessary for the provision of the service.

[42] E.g. age verification with regard to services for adults, see below 6.3.1.3.

6.3.1.2 Web pages for children and minors

The German data protection authorities also had to deal with websites which were specifically addressing children. In the case that was assessed, there existed possibilities of customising the site according to the children's wishes or to join special online communities. In order to use those features, the kids where required to enter in certain personal data. This did not only help the organisers to customise the site and to target their information, but also to prevent from unwanted access of paedophiles and other adult offenders.

When dealing with the issue it turned out, that in Germany as probably in most EU Member States, there existed no special regulations for processing personal data of minors. Therefore the data protection authority had to get back to general regulations. According to German Civil Law minors between 7 and 18 are granted a limited legal capacity, resulting in the need for parental consent for most contracts. However, with a view to the declarations of consent into processing their personal data, other principles must be applied, since such statements are not equal to genuine contractual declarations. What is relevant for the legal validity of a minor's consent in the field of data protection is his or her ability of comprehension; they must be able to fully understand the consequences of their action. This question has to be answered on a case by case basis. One important guideline is the fact that minors are granted the right to decide in matters related to their religious education from the age of 14 years on[43].

When dealing with these cases it turned out that a side glance at the USA was very helpful. Even though there is no general data protection act on the federal level in the US, for some areas of the private sector specific regulations do exist. One is the Children's Online Privacy Protection Act (COPPA) which entered into force in 2000. It applies to online services directed to children under 13 years of age that collect personal information from children. The most important provisions are the following:

- Provider offering content for the said target group are obliged to post a privacy information on their site.
- Moreover, they must ensure that a corresponding notice is given to a parent in an appropriate manner, e.g. via e-mail.
- Before actually collecting data, the web site operator must obtain verifiable parental consent from the child's parent.
- Moreover, they have to give access to the child's personal data at a parent's request.

These principles correspond to general data protection obligations in Europe and are not particularly surprising. The most difficult problem in this context is how parental consent can be obtained in a verifiable manner. Insofar, a lesson could be learnt from the US. The COPPA

[43] According to Art. 5 of the Act on Religious Education (Gesetz über die religiöse Kindererziehung) last amended 12 September 1990

regulations are being implemented by the Federal Trade Commission (FTC). After organising open discussions with all actors involved, the FTC has developed a so called 'sliding scale approach'. According to the latter, the methods for obtaining verifiable parental consent vary, depending on how the operator uses the child's personal information.

If the data was intended to be used solely for internal use, a measure is supposed to take place that could be called 'triple opt in'[44]. It consists of three acts to confirm the data collection which must be effected independently from each other. The fist two acts are equal to the double opt in required when subscribing to an e-mail newsletter, only that they must be effected not by the child but by a parent. At first the child who is supposed to be sitting in front of the computer is asked to call a parent who then must enter in his e-mail address and check a box indicating that he or she agrees with the data collection and processing. In a second step, a confirmation e-mail is being sent to the address. To continue the opt-in process, this e-mail must be sent back by using the reply function. To provide for more security to actually involve the parents and not only having the child itself operating all the steps, a second e-mail is sent after a certain time (ca. one week) to the e-mail address asking for another confirmation. Only after replying this second e-mail, the data processing may be carried out. The system apparently starts from the assumption that the child might be correct in entering in the parents e-mail but while sitting at the computer is able to reply to the first confirmation e-mail immediately by himself. The intention of the second e-mail is to make it more likely that a parent gets to see the confirmation in any event. When this system was implemented in the USA, it was consented with representatives from the different sectors who proved that the underlying scenario was a likely one. It goes without saying that the system would not work if the child entered in its own e-mail address. The assumption is, however, that at least smaller children would not hold an e-mail address of their own but use the parent's one.

In order to provide for an even higher grade of reliability of the parental consent, a different procedure has to be applied in cases where the data collected is to be disclosed to third parties or to the public. Since such a way of processing leads to greater risks for the privacy rights of the child, a written consent of a parent is required in those cases. The written consent may be replaced by a digital signature if this is regarded to be an equivalent for the written form according to the laws governing this field.[45]

As in the case that had to be decided by the German data protection authority the data gathered were only intended to be used internally for the adaptation of the service to the preferences of the child, it was agreed with the operators of the service to apply the triple opt-in approach.

---

[44] See above, section 5.2, on the requirements of a double opt in.

[45] More details can be found here: http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/index.html

6.3.1.3 Data collection in the context of age verification

Another problem closely connected to the one mentioned above is related to so called adult check or age verification (AV) services. Certain services on the internet are strictly limited to adults; minors shall have no access.[46] If such services try to comply to the laws, they must provide a log-in mechanism which effectively restrict access of minors. AV services strive to guarantee that an individual user who wants to log-on to restricted offers is actually of age. There are different business models existing, leading to more or less reliable age verification. The institution in Germany responsible for legal protection of children and young persons has developed criteria to assess the quality of such systems. In order to ensure secure authentication, at least one face-to-face check is required.

From a data protection perspective, it is important to organise procedures in such a way to comply with the principle of data minimisation. In order to achieve this goal, talks are currently being held between the institutions responsible and the data protection authorities.

6.3.2 Generalisation: Application of the basic principles of Dir 95/46/EC

6.3.2.1 Fair data processing principles

With a view to services as the ones described above whose business involves data collection via the internet, Dir 95/46/EC is relevant. As a consequence, in particular the following provisions of Art 6 of the Directive must be complied with.

Personal data required must be collected for a specified legitimate purpose and it must not be excessive in relation to that purpose, i.e. no unnecessary or irrelevant data may be collected. This can be doubtful in cases as the ones mentioned above where web forms have to be filled in forcing the data subjects to disclose more information than relevant for the purpose. The same is true for the obligation to register with the service in order to create a permanent account when only one single transaction is intended. Such practice conflicts with the obligation to delete data as soon as they are not longer relevant for the specific purpose as laid down in Art 6 para 1 lit e) of Dir 95/46/EC. From this provision it also derives that a storage period for the data collected has to be defined and applied.

6.3.2.2 Lawful processing criteria

Moreover, the processing must be in compliance with the lawful processing criteria laid down in Art 7 (and Art 8 were sensitive data are concerned). In the field of e-commerce, the provisions most likely to base personal data processing upon are:

---

[46] There is legislation in force in Germany defining more in detail which information is restricted for juveniles. Apart from information related to violence and pornography, some more recent examples comprised even some information (or rather: advertisement) on smoking, issued by a major tobacco company.

- Art 7 lit b), 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'. In the case of a contract or a pre-contractual relation, it is important to assess which data exactly is necessary in order to conclude and carry out the contract.

- Art 7 lit f), 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)'. There may be exceptional cases where this provision can be deployed as a legal basis for personal data processing. However, in most constellations of online data collection outside of a contractual relationship, it can at least be tried to obtain the user's consent. Therefore, consent as a legal basis should be preferred.

- Art 7 lit a), 'the data subject has unambiguously given his consent'. The statement of consent vis-à-vis an online service is effected by electronic means, naturally. Here the question might arise as to the technical features necessary to provide for a valid consent.

6.3.2.3 Excursus: Requirements for online declaration of consent

In Germany, the initial legislation, dating back to 1997, had prescribed the use of electronic signatures for the user in order to submit a valid statement of consent.[47] It turned out, however, that this regulation could not be complied with since in practice only an infinitesimal number of users were equipped with electronic signatures. The legislator reacted to that situation of factual impossibility and amended the law. The amended act has dropped the obligation to use electronic signatures.[48]

What is still required, however, is that the consent can be given only through an unambiguous and deliberate act by the user. In practice, a de facto standard is agreed upon, making sure firstly that for this purpose it is not sufficient to only click one button. To prevent from accidental clicking, at least two actions are required, e.g. checking one box and then clicking a button. Moreover, the consent must be recorded and the text of the consent must be made accessible for the user on request at any time.

---

[47] Art. 3 para 7 of the Teleservices Data Protection Act (Teledienste-Datenschutzgesetz, TDDSG) read as follows: 'Consent can also be declared electronically if the provider ensures that
1. such consent can be given only through an unambiguous and deliberate act by the user,
2. consent cannot be modified without detection,
3. the creator can be identified,
4. the consent is recorded and
5. the text of the consent can be obtained by the user on request at any time.'
It was agreed that in particular no. 2 and 3 can only be fulfilled deploying electronic signatures.

[48] Be deleting no 2 and 3, see amended Teleservices Data Protection Act as of 14 December 2001, Art 4 para 2, available online: http://bundesrecht.juris.de/tddsg/__4.html

In addition to this information obligation vis-à-vis the user regarding the mode of his consent, the general rights to information of the data subject apply. Consequently, the providers must cater for a system that clearly identifies an individual user in order to give access to the correct data subject. That can be achieved by furnishing the user with a user name and a pass word when he first logs in to the service. Many services enforce this by prompting the user to enter in such details when he places his order.[49] The log-in provided that way sufficiently secures that any information request will be answered towards the correct data subject. Such log-in data must not be retained for a period longer than necessary to perform the contract. Even though a comparable specific legislation is not in place in the Czech Republic, the underlying issues regarding the recognition of the user and the unambiguous and deliberate quality of the act of consent could be checked by the Czech data protection authority as well.

6.3.2.4 Processing criteria with regard to sensitive data

With a view to sensitive data in the sense of Art 8 of Dir 95/46/EC, any collection of data may be based on the explicit consent of the data subject (Art 8 para 2 lit a)). In specific cases, other exemptions according to Art 8 para 2 may apply. E.g. there may be special applications of trade unions or in the health sector, that rely on Art 8 para 2 lit d) or para 3. Such applications should be scrutinised particularly thoroughly. The protection of such special categories of data also requires a greater effort with regard to ensure the technical security of the processing operations (Art 17 para 1 second clause of Dir 95/46/EC).

6.3.2.5 Involving data processors

From the perspective of the content providers, in many cases one or more processors will be involved in both, the provision of the services and the data collection and processing. Typically, the content provider contracts an ISP responsible for the online publication of the content including maintenance of the e-shopping systems deployed. The ISP may engage a subcontractor who provides the web servers and connects them to the internet. A formal contract with the processor(s) has to be concluded, defining appropriate security measures and securing that data is only processed on the controller's instructions (Art 17 para 2 and 3 Dir 95/46/EC). It may be the case, though, that only the ISP has the technical possibility to access the personal data whereas the web server operator does not have it. In those cases, a contract in the sense of Art 17 of the Directive has only to be concluded with the ISP. With a view to the online processing of sensitive data (Art 8 of Dir 95/46/EC), special rules may apply. In Germany, health data entrusted to doctors are under a special legal protection of the medical professional secrecy as set forth in the Criminal Code; infringements amount to a criminal offence. The engagement of data processors when processing such data can not be based on the data protection act. In some Federal states of Germany there exist laws on the protection of medial data. Only these specific laws may serve as a legal basis for the involvement of data

[49] This should not be confused with the creation of an account as it has been criticised above. In the model described at this place, no other personal data are being collected. Only from a self-chosen user name and password, the service provider will not be able to relate information to a certain individual.

processors with regard to medical data. Where such laws are lacking, the engagement of processors may only be based on the consent of the data subject.

6.3.2.6 Rights of the data subject, information to be given

As mentioned above, all the rights the data subject has according to Dir 95/46/EC apply to online data collection. Therefore, it must be ensured that the right to access and to rectify can be exercised by the data subject.

Further on, in compliance, with Art 10 of Dir 95/46/EC when collection data online, all relevant information must be provided in order to achieve transparency for the data subject. This includes:

- Identity of the controller and representative,
- Purposes of the processing,
- Obligatory or voluntary nature of replies, as well as the possible consequences of failure to reply
- Existence of the right of access and the right to rectify the data
- Recipients or categories of recipients of the data
- Possible transmission outside the EU, indicating the safeguards

Basic information should be given prior to collecting data. In order not to overcharge the data subject, it is recommended to follow the approach of so called layered privacy notices. This implies to give some basic information on a first level, easily intelligible for the average user. A more detailed explanation should be offered on a second level for such users who intend to familiarise also with the detail of data processing. In addition, it is recommended to include a link on each single page of the service that would lead users immediately to the page where the basic privacy information are being provided.

6.3.3 Additional features: cookies

Cookies were originally designed to facilitate the use of web services that are used over a longer period of time or with a certain frequency. Such services, as e.g. online shops, can utilise the technology in order not to lose customers when they are clicking their way through a web site. Due to the deployment of dynamic IP numbers as explained above, a certain user might be allocated a different IP number by his IAP after a certain period of idleness. If this happens, the web server would be incapable of recognising the user unless additional technologies such as cookies are applied.

6.3.3.1 Underlying technology

Technically speaking, cookies are a small set of data that is being stored in the computer of the user triggered by the web server when visiting sites that use cookie technology. Depending on the browser the user deploys, the cookie data can be found either in the file ‘cookie.txt’ (Mozilla and Firefox) or the cookie directory (MS Internet Explorer). With the next visit to the domain that has set the cookie, it is being retransmitted from the user’s computer to the domain server; thus a certain user can be recognised by the web server. Cookies can be retransmitted to a server within a certain time period, depending on the programmed cookie life time. Life time may vary from a few minutes to many years. Whilst so called session cookies are not being stored to the hard drive and are only active until the browser is being shut down, many cookies have a programmed life time up to the year 2038 - and thus probably much longer than the computer they are stored on.

What is most relevant from a data protection perspective is the fact that cookies can not only be set by the URL chosen by the user (as www.lycos.com), but also via banner ads on web pages and any other element that is opened with a web browser and has the possibility to connect to the internet.

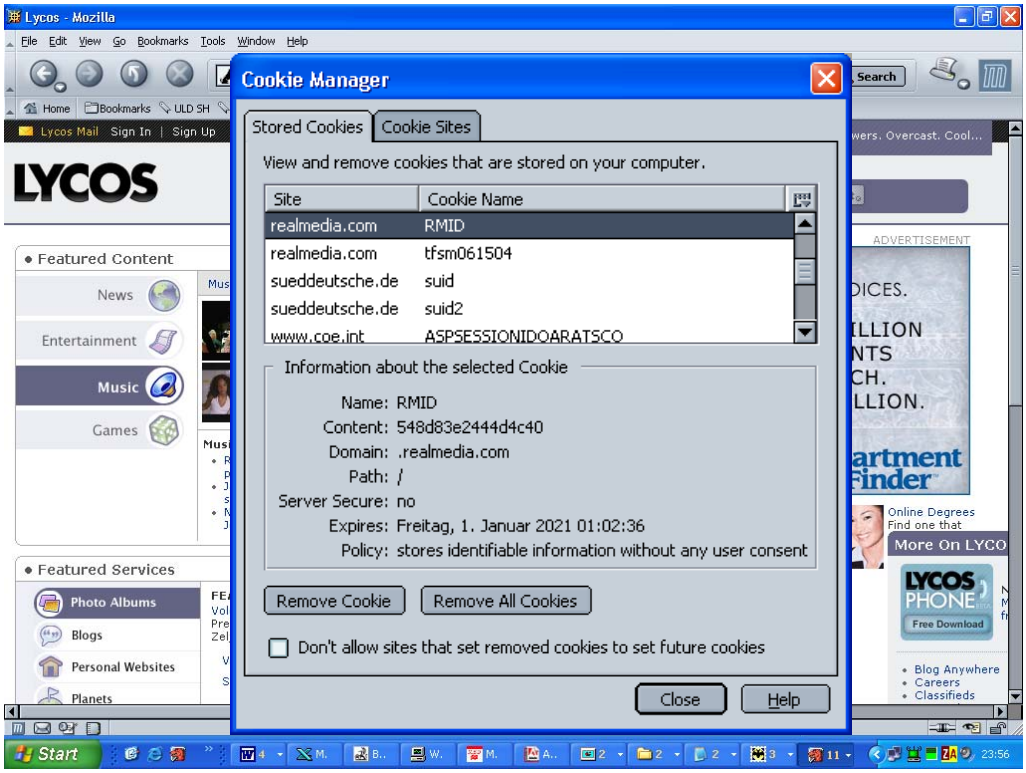


Figure 5: When opening the URL www.lycos.com, a cookie from a different domain is being set

The consequences of this technology are obvious: Computers (and thus potentially users) can be marked when entering a web site, so that with a follow up access they can be distinguished as the user (computer) who has visited the domain before at a certain date and time, additional information could be added as special preferences, previously ordered goods, etc. If the web

server operators were able to gather sufficient information, possibly analysing several site visits over a longer time period, they could even create a profile of the user.

6.3.3.2 Legal regulations, lex cookie

It depends on the decision discussed above regarding the quality of IP addresses as to whether or not the information collected by means of cookies must be regarded as personal data.[50] If the strict approach described above is followed, it might occur that user profiles were created without coming to the conclusion that personal data was existent. It has to be borne in mind, however, that the situation may change rapidly with just another bit of information being collected, leading to the possibility to relate an existing set of data to a natural person.

But even in the forefront of processing personal data, Dir 02/58/EC contains a regulation targeted at cookies and kindred technologies. Art 5 para 3 reads: 'Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/ 46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.'

Applying this regulation to cookies, it can be found that the exemption in the second clause permits the setting of session cookies and cookies with a very short life time (hours) which only serve to enable a certain feature of the site. In addition, the exemption might also apply to cookies which serve to recurrently admit the user to a long term services (e.g. subscription of an electronic newspaper) as long as this forms an essential part of the service requested by the user. It must be pointed out, though, that the exemption does not apply to third party cookies and cookies only solely set for proprietary purposes of the service provider himself (e.g. tracking the click stream of site users).

Where the exemption does not apply, the lawful setting of persistent cookies requires respective information of the user which also must have the right to refuse the cookie. The legislator of the Directive, however, intended to impose an obligation to duly inform the user in any case, as can be seen from recital no. 25: It is required that 'users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using.' In the cases of the privileged short termed cookies, this requirement can be met with a general information on the web site of the service. With a view to the other cookies, a previous information is mandatory. As can be seen from many

[50] See above, section 2.2 and section 3.3.1.

examples in the wild, this provision of the directive and the national laws is scarcely complied with.

7 Application layer – conveyance of content – obligation to confidentiality

Confidentiality of communications conveyed through electronic communication networks is protected by Article 5 of Dir 2002/58/EC and by Art 8 of ECHR as interpreted by the European Court of Human Rights.[51] As a general rule, storage and other kinds of interception or surveillance of communications and the related traffic data are prohibited. Exceptions apply to lawful interception of communication carried out on behalf of law enforcement agencies and intelligence services. Moreover, the mere technical storage necessary for the conveyance of a communication is permitted, without prejudice to the principle of confidentiality.

One practical consequence with regard to e-mails is the prohibition to retain any data relating to forwarded e-mails on relay servers in the internet; all data must be deleted after forwarding the e-mail. In case the forwarding turns out to be technically impossible, the e-mail may be stored for a short term in order to retry. If it fails either, an error message may be returned to the sender and the traces of this communication have to be deleted on the servers involved. After the e-mail has arrived at the mail server it was destined to, storage on that server is permitted only until the recipient fetches the mail. Unless different settings were chosen by the recipient, the e-mail provider is obliged to delete the e-mail on the server once it was downloaded by the recipient.

Another issue discussed in the context of confidentiality is the deployment of anti-virus tools which are scanning the e-mails sent via the technical facilities of e-mail providers. If on a technical level virus scanning is being executed, sufficient safeguards must be implemented in order to secure the confidentiality of the message conveyed.[52] It is important, e.g. to guarantee that the message is not being read be humans. It is permissible, though, to delete the virus (and the message if necessary). In any event, notification should be sent to the recipient and the sender.

In this context, also sniffing is discussed. It comprises the monitoring of traffic on a network, using so-called sniffing software which allows to look for certain characteristics, typically the presence of predefined keywords. Such intrusion into the confidentiality, carried out in a public communications network or publicly available electronic communications service would amount to an infringement of Art 5 para 1 of Dir 2002/58/EC unless it was conducted by government agencies who are specifically entitled to such measures, carried out in

---

51 See above with regard to confidentiality implementation on the TCP/IP layer, section 3.2.4.

52 See also WP 118 as of February 2006 of the Art 29 working group which comes to identical conclusions. A more general question would be whether the mere technical control of content that does not lead to any human taking note of the content amounted to an encroachment on somebody's rights. This question can not be discussed here in full extent but only pragmatically denied.

accordance with the conditions imposed by Article 8 of the European Convention on Human Rights.

With a view to controls by data protection authorities, it is not only relevant to evaluate whether any infringements are currently taking place. It is of the same importance to verify that appropriate technical and organisational mechanisms are in place in order to prevent any disclosure of content.

8 Location based services

Recently German data protection authorities were concerned with location based services offered to the wider public. Whilst in a commercial environment sophisticated tracking techniques are already in use (e.g. for so called fleet management, i.e. overseeing the movements of all vehicles belonging to a company), they eventually emerge in the consumer sector.

8.1 Underlying technology

Location based services can work on different technical protocols. Whilst the mobile network providers are having access to some more basic location information in the context of their network operations, additional tools, based on GPS signals, are able to provide more precise information.

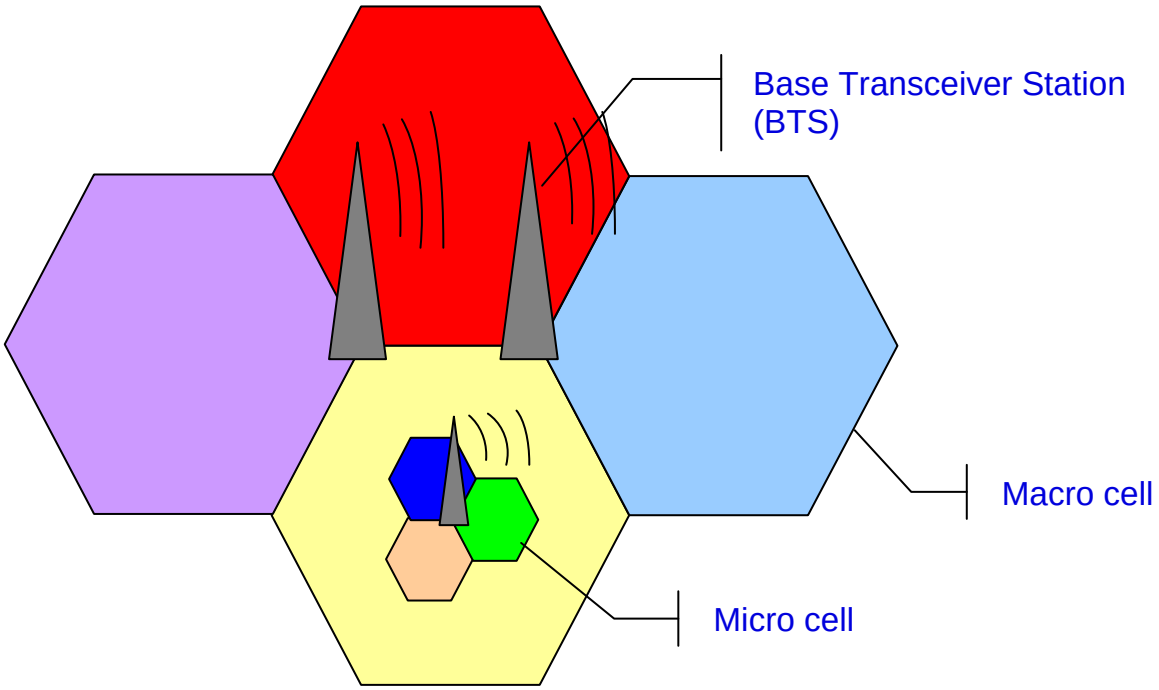


Figure 6: Location data available in the mobile phone network

As a side effect of the standards used in mobile networks, the providers may on a technical level record and store information on the mobile phone cell were incoming and outgoing calls were received by their system. In a mobile network, the identification of a Base Transceiver Station (BTS) is processed in order to enable the conveyance of communications. The BTS handles the calls in a certain mobile network cell. Depending on the environment (city or densely populated areas), cells may have different seizes, ranging from some hundred meters to some kilometre in diameter. In a legal sense, the BTS identification can be regarded as location datum and traffic datum and may be processed in accordance with rules on traffic data.

In order to provide location-based services, in many cases more precise location data (not only the network cell) are necessary, e.g., measurement of the angle of arrival of the signal at the BTS and measurement of the time of arrival of the signal at the BTS (to estimate the distance to the BTS) etc.

If the mobile device is equipped with additional features like a GPS receiver, more precise information may be used on the application layer. In order to realise such services it is crucial, however, that the positioning signal received by the device is being conveyed to a central system which then analyses it. Such services are normally used in the context of fleet management as mentioned above and other tracking applications for vehicles.

8.2 Recent German case: friends finder

In Germany, the service provider AOL in cooperation with a major mobile network provider was planning to offer a service called friends finder. Users subscribing to this service would offer to their friends who also participated in this service the opportunity to track their current location via mobile phone and a web front end. The user interested in his friend's location would enter in a respective request on the web or possibly in the future on a web application on his mobile and would then receive the respective information, generated from the BTS information, processed and conveyed from the mobile phone network.

From the beginning, those services were intended to be strictly based on the consent of the user. However, in practice, some details appeared to be more complex than originally estimated. What was crucial from a data protection perspective was to provide for transparency for the user who was to be tracked. It was intended to offer the possibility to switch the service (or the trackability) on and off by sending a text message to the provider. Nevertheless, a lack of transparency was still noted since it might not have been obvious to the user that the tracking mode was still enabled. Thus, the idea was discussed to inform the user each time a tracking was requested by a friend of his, sending a text message to the user's mobile equipment. From a data protection perspective, such information could be regarded to be sufficient if it was given prior to disclosing the location to the requesting user and thus enabling the mobile phone user to reject on a case by case basis to be tracked (see below).

8.3 Specific legal regulation

Dir 2002/58/EC contains special regulations for location data. According to the definition given in Art 2 (c) 'location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

Art 9 para 1 sets forth that 'location data may only be processed when they are made anonymous, or with the consent of the users to the extent and for the duration necessary for the provision of a location based service.' Moreover, 'the service provider must inform the users, prior to obtaining their consent, of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.'

What is most important with a view to the users rights and to transparency is the provision enclosed in Art 9 para 2: Even where a general consent has been obtained from the user, he or she must 'continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.' From this provision the requirement derives for friends finder and similar services to inform the user on a case by case basis and to offer the possibility to opt out for each single process of being tracked.

It is well understood that from the general requirement of obtaining informed consent there originates the obligation of the provider to inform users, prior to obtaining their consent, of the type of location data which will be processed, purposes and duration of processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Finally, Art 9 para 3 defines that processing of location data must be restricted to persons acting under the authority of the provider and must be restricted to what is necessary for the purposes of providing the value added service.

Even though these regulations can be regarded as a privacy friendly legislation, one aspect must be borne in mind. Art 10 lit b) obliges Member States to ensure that there are transparent procedures governing the way in which a provider may override the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls. In practice this means that e.g. emergency units shall have the possibility to find injured people after an accident even though they have switched off their location based service.

Insofar, apparently a compromise between the right to privacy on the one side and public safety on the other was struck. There is still one technical problem, though: In order to implement this provision, location data must be transmitted out of user's device to the

telecommunication provider in any case. The consequences are that the users do not have exclusive control over their location data. The obligation cited above applies not only to providers of a public communications network but also to providers of a publicly available electronic communications service. This would also include providers who base their services on other information than the BTS info generated by the network. Even services based on GPS are included in the first place. However, in practice, with regard to GPS based services, there will still be the possibility for users to decide in any case whether data on higher protocols are being conveyed since the provision cited above is an obligation imposed on the providers, but not yet a design criterion for mobile devices. In other words, it should still be possible to simply switch off such services at the mobile device where the precise location information is being conveyed on the application layer. In contrast, the location information received by the mobile phone network will be always on.

Annex 1:
Reference list regarding possible aspects of data protection controls in the field of e-communication

Annex 2: Abbreviations

ADSL	Asymmetric Digital Subscriber Line
BTS	Base Transceiver Station
CISSA	Czech Certain Information Society Services Act
Dir	Directive
DNS	Domain Name System, also: Domain Name Server
ECA	Czech Electronic Communications Act as of 22 February 2005
FDPA	German Federal Data Protection Act (Bundesdatenschutzgesetz)
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IAP	Internet Access Provider
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
NAT	Network Address Translation
NIC	Network Information Centre
PDPA	Czech Personal Data Protection Act as of 4 April 2000
POP3	Post Office Protocol version 3
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
URL	Uniform Resource Locator

9 The basics of e-Government

State-of-the-art information and communication technologies make it possible for public administration to provide electronic services through the Internet allowing these new e-Government services to better serve the needs of users. The Internet makes finding and using these services easy and comfortable and in most cases it is not necessary any more to go to a Government office. The offered services are provided electronically, regardless of time or place.

However, it is important to point out that Internet use to provide administrative services is a possibility, not a must. E-Government is an alternative, not an obligation. For all those who prefer personal contact with authorities or who are not yet completely familiar with the new media it is still possible to conduct business in the familiar surroundings of an office concerned. However, e-Government is also beneficial for this group of people because e-Government can deliver faster results even when employing conventional official channels.

9.1 What is e-Government?

By offering electronic services, the authorities provide the users with comfortable access to public administration. From the authorities´ point of view, the use of information and communication technologies for the provision of electronic services implies considerable internal organizational changes and challenges. The processes have to be partially remodeled and operational procedures have to be adapted to new requirements. The development of administration operations will increasingly be performed using automated procedures. As a consequence, the officials will need to acquire necessary knowledge and skills to be able to use the deployed technologies. E-Government comprises all these elements.

On the EU level, e-Government will be defined as

"the use of information and communication technologies in public administrations combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies".[53]

9.2 E-Government in Austrian authorities

After reassessment of the federal IT-strategy in 2001, considerable progress has been reported with regard to the development of e-Government. A number of administrative operations can already be completely performed on the Internet. In this respect, a fundamental role of e-Government is its by sustainability, security and data protection considerations.

[53] Communication of the European Commission to the Council, European Parliament, European Economic and Social Committee and the Committee of the Regions "The Role of e-Government for Europe's Future, COM (2003) 567 final, 26.9.2003, Commission of the European Communities, http://europa.eu.int/information_society/eeurope/2005/index_en.htm

A sustainable e-Government can only be successfully implemented on the basis of a comprehensive strategic concept. The Austrian e-Government strategy stipulates basic concepts, elements and standards which serve as guidelines for the implementation of a range of electronic services and infrastructure.

The e-Government strategy should be understood as a plan and guideline which enables a continuous development and extension as all as a permanent adjustment of technological conditions (Change Management). The proposed partial strategies, policies, measures and initiatives are part of the manual provided information over minimum standards and obligations which have to be complied with and which make together make a homogenous complex unit. Basic principles and considerations for an integral architecture are embedded into the strategy.

By means of buzzwords such as Citizen Card, electronic signature, portal network, electronic delivery, security or electronic payment it is easy to realize the variety of building blocks which shape the Austrian e-Government.

Despite of considerable progress and success compared to the international arena the development of a comprehensive e-Government can by no means be considered as complete. The evaluation, spreading and implementation of strategies require constant efforts and innovation in order not to give up the acquired gains. Although the elements and concepts already available are rather comprehensive new elements and fields, e.g. electronic participation of citizens, are constantly being added to the concept.

The continuous evolution of e-Government has to remain straightforward and transparent. It has to be taken into account at all stages of strategy implementation in this field that services as such concern individual citizens and thus have to be user-friendly and applicable without much effort by any average citizen. To a large extent it is a precondition for the acceptance and success of such a concept. In the next part, both organizational and technical basic principles will be presented.

9.3 Concept

The use of features which e-Government has to offer should not be hindered by either local situation of affiliation to any given group in need of these services. Whenever possible and justified, known technologies such as cell telephony should also be used. Only complete availability to all, without any discrimination and need of special skills, may implement the concept of more responsiveness to the needs of the public more widely. It comprises also access through an intermediary, i.e. a person who can intervene on behalf of those citizens who don’t want to or can’t use a computer.

Electronic services provided by public administration should be attractive for all users. The demand of being available to all requires a simple design. The main objective followed by the course of procedure development should concentrate on optimation of convenient usage.

Comfortable access will increase the readiness of users to resort electronically offered services to a larger extent.

In order to eliminate all local barriers to access an efficient civil service has to aim at comprehensive electronic introduction, including payment and delivery possibilities. In order to eliminate inhibitions felt by users, uniform interfaces and uniform designs should be used consistently.

One of the main objectives of e-Government is increased efficiency. As a consequence, implementation work has concentrated, along with the creation of infrastructure, on integrated procedures which will be used rather frequently. This is particularly true for procedures in the field of finance, justice or economy.

In Austria, electronic files and resource management, as well as the portals, represent the fundamentals for an efficient back-office and thus for electronic procedures oriented at individual transactions. The higher the level of readiness to use electronic administrative services intensely the better is the chance that the administrative system will function in an efficient way.

The administration will assess cost efficiency in order to decide whether to make the procedure automated internally, using electronic acts, or an integrated application. With the exception of speed implications, the decision will have no effects on citizens since they will still be able to use electronic services even in cases when the necessary procedure is still performed in a conventional way (manually).

Successful e-Government is founded on the following three main pillars:

1. A clear legislative framework that is easily accessible and therefore becomes quickly familiar to those concerned.

2. Safe and therefore sustainable systems and services as a prerequisite of its broad implementation and the strengthening of citizens' confidence in electronic public administration services.

3. The application of sustainable technology based on open standards and defined interfaces in order to ensure permanent adaptation to new technologies.

Help.gv.at has been successfully established as a contact point for administrative procedures in Austria in the past. Using a single user interface, forms from a whole range of fields have been and will be provided along with corresponding explanation and hints for their completion. The development of the interface into a transaction portal, based on a clear strategy, should lead to an optimum availability of services provided to citizens.

It is only possible to achieve sustainability by the use of international standards and open interfaces which are applied across all producer borders. This should create a basis for cooperation of different systems and organizations. The use of open interfaces and standards

not restricted to individual providers will correspond with Austrian economic structure consisting predominantly of small and middle-sized enterprises and may thus lead to strengthening of Austrian economy. The initiative “Open Source E-Government“ will increase economic performance which, with the same amount of resources, will consequently exhibit higher competitiveness due to the fact that current elements can be further built upon which will lead to decreased development costs.

9.4 The actors of e-Government

Within e-Government, there are different communication relationships with regard to those involved in electronic communication. Classic administrative procedures which can be carried out between the administration and individual citizens are referred to as “Government to Citizen” (G2C) communication or transaction. Should the same procedure be performed between the administration and companies it is referred to as “Government to Business” (G2B). Data exchange between individual authorities are defined as „Government to Government“ (G2G).

9.4.1 Public administration

In a country with a rule of law, public administration has to fulfill its statutory duties. From the sociological and economic point of view it always has to bear in mind common public good. Therefore, based on legal requirements, public administration has to provide certain services to the citizens. The citizens will therefore be increasingly regarded as customers, not applicants. Using new communication technologies, the administration can better comply with the requirement of service orientation.

The use of new media technologies reflects also the openness of authorities towards innovation which has positive effects on its image in the eyes of the public. The provision of services by means of the Internet is a sign of service orientation of the authorities with respect to citizens who would like to settle their matters using this medium.

An increased use of information and communication technologies in public administration should lead to a shorter file processing time thus making the services faster. The process organization should be improved and better structured in the course of the implementation of these technologies by analyzing individual processing steps with regard to the New Public Management. By removing organizational overlapping and automation of office processes a more effective and efficient working method will be achieved. In addition, the structured electronic data landscape will enable to access saved data faster and more accurately. On the one hand it is possible to protect the data stored with the authorities from technical and organizational point of view; on the other hand they may be processed with regard to data protection legislation. It is therefore necessary to ensure that data will protected against an increased risk of their fraudulent use by making it impossible to illegally access the data.

In the medium and long term it is expected that the abolition of the need to provide manpower in administrative offices which was occupied by registration, archiving, transportation and dispatching of paper files will lead to cost saving and at the same to an increase in productivity. Presently, the first experience demonstrated that the implementation of e-Government in Austria has led to enormous savings with regard to office supplies. The savings in personnel will be delayed because the implementation of e-Government and familiarization of civil servants with the new professional environment was rather labor-intensive.

9.4.2 Citizens

In their everyday lives, citizens may need some services provided by public administration. Often, their personal or business lives depend on these services which can only be obtained from a certain public authority[54]. From the point of view of those involved in e-Government, businesses are to be treated in the same manner as citizens, the only difference being that of the better access of businesses to the Internet, better IT infrastructure or more frequent contacts to administrative authorities. Therefore, the term "client" is commonly used both for citizens and businesses.

If the citizen of the business has a request with regard to an authority he/she expects to be treated fairly. Using new media (first of all e-mails and Internet), the contact with authorities can be provided independently of time and place. Moreover, all necessary steps can be performed by only one contact of the citizen with the authorities. This should also be true when several administrative offices or bodies are involved are or have to be dealt involved. Using the Internet, the citizen also has a possibility to trace the status of his/her affair.

It seems that the achievement of the objectives of simplification, speeding up and transparency presents a significant improvement of the way public administration works.

The objective is to provide the citizens with a possibility to manage their business with regard to public administration on-line seven days a week around the clock. It is possible to achieve it by means of the Internet. New communication channels (e-mail, on-line forms) make it possible to submit applications independently of time and place. This way, the citizen is spared the need to go to the authorities several times, as well as to lose time waiting in lines. First of all, if the citizen has an Internet access he/she has a possibility to deliver his/her applications any time and from anywhere. Clear relatability and the possibility to trace back individual procedure steps lead also to the increased transparency of the entire administrative process. From the citizen's point of view, shorter delivery channels make the procedure shorter and his/her comfort is considerably increased due to saved time and effort.

---

54 In case of punishment, the citizen would rather avoid any contacts with the authorities.

It has to be borne in mind that clients have to have a certain technical infrastructure (computer, Internet access, signature chip card, card reading devices, etc.) in order to be able to use the provided advantages. These costs are to be borne by the clients. However, there is a range of political initiatives aimed at promoting the purchase and use of these means (tax deductibility of broad band Internet access[55], no fees for using a "Citizen Card"[56]). Therefore, it is to be expected that the full use of e-Government will be achieved in the medium term when public administration is able to provide a wide range of applications and the technical means available to customers become as widespread as expected.

9.5 A graded system of forms

In order to provide a better overview of different interaction levels, we distinguish the following three types of electronic services:

- Information services;
- Communication services; and
- Transaction services

which can be applied in individual fields to contact authorities or achieve political participation.

Basically, these forms build on each other from the point of view of their development, implementation, maintenance and their everyday use, as well as from the point of increased usefulness derived from each service both for citizens (clients) and administrative authorities. It results in higher requirements on: information services with regard to the possibilities to use new electronic media, communication services which enable a considerable exchange of information, and transaction services which, as the most-advanced services, should lead to the achievement of the objective of fully electronic management of administrative processes. It is not necessarily true that the functioning of one level is dependant on the functioning of the next lowest level; however, the complex nature of the e-Government project under development requires structured approach based on previous experience. Each of these types of services is not only based on legal, technical and organizational general requirements but also leads to a complete and comprehensive reorganization of all these services.

The analysis of international developments in the field of e-Government suggests that information services (government agency help site, important general information, legal information, etc.) at present represent by far the largest part of offers, while communication and transaction services have an enormous growth potential. Communication services used to deliver electronic messages for authorities or public officers (mostly e-mails) present new

[55] Article 124b Z 81 of the Income Tax Act 1988, Federal Code l. No 400, as amended by Federal Code l. I No 71/2003.

[56] Article 10 of the Fee Act 1957, Federal Code l. No 267, as amended by Federal Code l. I No 10/2004.

requirements to be fulfilled. Transaction services with regard to administration, e.g. electronic applications, tax returns, seem to be especially beneficial due to their potential to simplify the provision of administrative services leading to more flexibility and time saving. As a rule, their implementation is on the other hand related to a number of prerequisites concerning security and regulations.

The One-stop-principle seems to be a procedure to follow within the provision of electronic administrative services. It enables the client to manage his/her affair, in which several administrative offices and/or several levels of administration and/or private service providers are involved, from one contact point by means of electronic support.

9.5.1 Information services

It is generally known that the flow of information provided by the Internet is virtually hard to be overlooked. It is not always easy to filter out the correct or important information; however, the advantages of acquiring information and knowledge completely independently of time and place are worth all efforts. The State and its administration should and have to participate in the provision of information within the framework of legal data protection. It makes the administration more accessible to citizens and increases their comfort. The Internet seems to be the most suitable means for the provision of relevant information.

At the beginning, the authorities have to select which data may be useful for citizens. The authorities often confine themselves to their own presentation which may be reasonable and motivating for their staff members but which does not bring very much to the user of such a website. A list of staff members displayed in addition to the address of an authority can't be really that useful. Information which should be provided to citizens on such a website should generally clarify the rights and duties of citizens presented in a reader-friendly "lawyer-free" language. As a result, instructions should be provided which describe how to achieve that one's affairs are satisfactorily dealt with by the relevant authority. This system based on so-called "Lebenssachverhaltsprinzip"[57] (a so-called "principle of life circumstances") was designed to fulfill the needs of the citizens at best. In comparison with an information brochure published exclusively as a paper copy, electronic media provide a number of advantages. The contents of such a brochure can be updated faster and without any significant additional expenses. Their availability is to a certain extent unlimited and in combination with other documents widely diversified with regard to information provision. On the other hand, due to available possibilities, users of these services also have higher expectations concerning the updates. This is a challenge which has to be addressed by any customer-oriented authority.

With regard to data protection, access to such general information does not require an access protected by means of any client identification. As long an and authority does not provide any

[57] Under this term, official procedures related to a particular life situation are understood. Provision of information and access points are not classified according to different responsibilities of authorities but according to different life situation, e.g. wedding, driver's license or military services, which leads to a more efficient and transparent grouping of the affairs.

personal data - like consulting a register containing personal data - any such information may be freely available.

The advantages for authorities lie in that all the parties are given more information. It should lead to the situation when authorities are not contacted personally with general everyday questions and the parties can receive all necessary forms and data upon the first contact. Thus, a relatively simple use electronic media is a step in the right direction leading to a more efficient distribution of human resources and faster administration.

If we compare information services with services which are technically on a higher level, their provision seems to be a relatively easy task. The efforts are much lower due to one-way communication. The authority does not have to, or can't react in any specific way within the framework of information services. The data are only stored in the network in an understandable manner. At the very least, it is necessary to provide the above-mentioned updates. With regard to data protection, it has to be ensured that information provided is updated and correct and can't be manipulated by a third party.

9.5.2 Communication services

This form of e-Government is based on the idea of a two-way communication system. Individual customers have a chance to ask particular questions through electronic media or to seek contact from a certain public officer. Since, as a rule, only general information about administrative procedures are provided this way, which means that there is no legally binding effect, all means which are available in the Internet, e.g. chats or newsgroups, may be used. However, the main use in this case will be of e-mails, which is the most-used application by those interested in these services. However, if there is insufficient information or insufficient FAQs[58] provided on the homepage of an authority, it may only involve a shift between telephone and e-mail requests.

Apart from that, request forms - preferably in an unchangeable PDF format - may be provided to be downloaded from the website. These will be printed out by the applicant and, after completion, sent to the authority concerned using regular mailing services. Similarly, electronic forms which may be completed may be evaluated online or by using a PC. These should also be printed after completion and delivered by mail. It is also possible to deliver the forms in person; however, it is only recommended for procedures which require it. The identification of an applicant, if necessary, is performed by means of his/her personal signature or, in the case of a personal contact, by means of a picture ID. Electronic signatures are not employed at this point.

This way, the authorities save the costs of printing at the expense of customers. In addition, the amount of forms is governed by the exact needs of applicants. However, since paper forms are still used by authorities to a large extent, at least during the unavoidable transition phase,

[58] Under „Frequently Asked Questions" (FAQs), a collection of frequently asked questions concerning a certain issue and the answers provided to these questions is understood.

this cost reduction is relativized. Due to significantly higher implementation requirements, the electronic transmission of forms is part of transaction services.

From an organizational point of view, communication services mean that the authorities have to provide a person who will monitor incoming e-mails and answer the questions. It may possibly lead to the need to higher labor costs.

When sending e-mails, due respect should be paid to invariability of the message. While the information provided is not of a legally binding nature, it is not possible to rule out official liability of authorities which provided a falsified piece of information leading to a negative administrative decision with regard to a party concerned. It is, therefore, not possible to view communication services only from the cost-benefit point of view, rather it should be considered as service provided to customers.

In addition to contacts with authorities, political participation also represents a huge potential for the use of these services[59].

9.5.3 Transaction services

The ultimate aim of e-Government projects should be a fully-fledged electronic processing procedure. The procedure between authorities and their users is called a transaction. This high specificity should be achieved by means of transaction services which mostly involve the provision of a paper document by authorities. Thus, applications should be first completed on-line and then delivered electronically by means of a website form or e-mail. The completion of the service by authorities, most commonly in the form of notification, will again be sent to the party electronically.

In order to achieve the operation of the system it is necessary to bear in mind that it is related to a number of technical, organizational, legal and other factual aspects which will require a considerable reorganization of the authorities. Internal processing has to be adapted to electronic contacts with the citizens, which requires investments into IT infrastructure and a corresponding training of staff members. On the other hand, there is a question posed by the applicant about how to sign the form or possibly append any annexes.

The demand of the citizens related to the possibility of carrying out administrative procedures using the Internet is rather significant, with clear benefits for any potential clients. Thus, employed people can deal with the office hours of administrative bodies which are often quite unfavorable and use the Internet independently of the time. Technically speaking, the Internet provides an unlimited access worldwide, not only in a particular office, which provides additional independence of the place and flexibility and spares time-wasting trips to the office. It means that authorities who might only have a seat in the capital get much closer to the citizens, especially those living in the country. Finally, there is the hope that using new

[59] E.g. *Nadjafi*, Participative legislation in the Internet, in *Wimmer* (Hrsg.), Quo vadis E-Government: State-of-the-art 2003, proceedings of the second E-Gov Days of the e-Gov.at forum, 255ff.

technologies will lead to a faster provision of services. Transaction services are appealing to public administration due to their potentially lower costs. They should lead to the situation when paper logistics, superfluous in the case of fully electronic file management, will become unnecessary and an automatic documentation of files will be achieved. The individual processing steps which will remain unchanged can thus be made more effective and faster. On the other hand, it requires the above-mentioned investments which will only be paid off later.

Judging by the complexity of transaction services, it is to be expected that their implementation is a protracted process which depends on a whole range of factors and requires a concerted interplay.

Despite the fact that e-mails are rather easy to handle, in reality, there are many problems which result from the issue-related communication between the customer and administration. The abundance of e-mail addresses, also with regard to authorities, makes it difficult to find the appropriate office. Should an e-mail request get to the wrong e-mail address, the risk of its further transmission remains with the client. It is only rarely that the sender is informed about the arrival of his e-mail. Automatic arrival confirmation is usually only compatible with the same mail software. It occurs in many cases that an e-mail does not reach the relevant authority because it was previously sorted out by a spam filter because it contained an application. Finally, a reliable verification of the contents of an e-mail, as well as an identification of a sender, is only possible by means of an electronic signature. These reasons led to a strategy in Austria to focus more intensely on on-line forms.

On-line forms are forwarded to relevant offices according to their topic using a predefined addressing system. Their arrival is documented by means of an acknowledgement of receipt provided also to the sender. It is not related to any transmission risks for the sender because he immediately knows whether his application has reached the right authority. Therefore, e-mail spamming has been done away with both with respect to authorities and to applicants. For e-mail forms, the authenticity of an application, as well as the identity of an applicant is verified, should it be required with regard to the application, by means of an electronic signature, or a Citizen Card feature.

In Austria, a recommendation valid state-wide was established for the development, structure, individual elements of the forms (addresses, fees, etc.) and design in order to ensure the recognition and uniform lay-out of official on-line forms. This styleguide[60] does not only help to create a uniform look and feel but also ensures simple usability and functionality of the forms. And finally, the development costs are only incurred once by the authorities because the existing building elements and procedures can subsequently be used repeatedly.

60 http://reference.e-government.gv.at/Styleguide.299.0.html

9.5.4 One-stop services and portal

Information and services provided by public authorities have to fulfill certain quality criteria: they have to be reliable, trustworthy and openly accessible. Internet portals are used for making electronic administration accessible to citizens and businesses.

There are many cross-sectional affairs known to the legal system. Therefore, it is often necessary to make several applications in order to deal with one single matter (life circumstances). With regard to the citizens, however, it should be possible to achieve it by means of a simple request. The authorities have to check special procedures with a view to different aspects, in particular building projects, motor vehicle registrations, or military draft procedures. However, for the citizen such an event is still considered to be a single unit/occurrence. The citizen is not familiar with the number of authorities which are involved or, in fact, feels that they constitute a cumbersome barrier. In order to ensure a consequent application of the principle of life circumstances, the authorities should establish a single contact point[61] which should combine the above-mentioned main forms and points dealing with one type of affairs. Using the so-called one-stop service, the customer has a real possibility to achieve all necessary steps with only one action. Basically, he does not have to notice any procedures which are initiated by his request. Therefore, no previous knowledge related to the structure of the public sector is necessary.

The combination of all the materials can be performed horizontally, encompassing several administrative offices, or vertically, comprising several levels of administration, such as the federation, provinces (Länder) or municipalities[62]. Implementation problems mostly arise during the networking and integrating the entire spectrum of public administration. In order to solve the issue, it is simply necessary to implement administration reform measures, e.g. bundling of administrative responsibilities. Another approach is the virtual one-stop services which functions by means of ICT. Therefore, a uniform Internet access site is an option. A so-called portal will be used to provide information and services of different institutions using a central website.

The portals are divided into several levels of development according to their functions. With regard to the services provided, the portals are classified into purely information portals, information portals having a binding character (e.g. binding legal information systems) or administrative transaction portals.[63] For efficiency purposes and in order to ensure cost saving synergies, portals should be designed first of all with regard to aiming target groups.[64] Relevant special portals are still waiting to be developed. The adaptation to the technical skills of users can also increase the acceptance and usage of the portals.

---

61 The contact point can be established as a real office available to the public or as a virtual Internet portal. For citizens without Internet access, the portal service can be provided in a publicly available office.

62 *Aichholzer/Schmutzer,* Bericht/Information E-Government - Elektronische Informationsdienste auf Bundesebene in Österreich, a study performed on behalf of the Federal Chancellery, 22.

63 *Gritschenberger/Schulz/Wimmer*, Portale und Bürgerdienste, Part 2, Computer kommunikativ, 5/2002, 14.

64 *Gritschenberger/Schulz*, Portale und Bürgerdienste, Part 1, Computer kommunikativ, 4/2002, 37.

The citizens - as customers using public services - should be provided with a system independent of the authority in question which would be accessible by means of a global Internet contact point (a portal). Thus, the user will be offered, with much commitment, a unit which virtually does not exist but functions as such thanks to its internal structure and harmonized workflow. The real complex structure and design of public administration does not appear clearly and remains invisible for the citizen. In this respect, the complete process integration comprising access to the portal, media-break-free management and archiving, as well as electronic delivery, constitutes the highest level of portal implementation as far as its complexity is concerned. The most difficult part of the performance of administrative procedures which should be carried out by means of such portals as part of the provision of transaction services is the integration of mostly existing and separately developed e-Government applications. Therefore, it is first necessary to achieve compatibility which is virtually non-existent.[65] However, the request specifics are significantly higher than within a single administrative office due to the interoperability of unequal transaction services in all areas (technical, organizational and legal) without guaranteeing the possibility to achieve cost savings as compensation. Thus, the portal serves as an entrance to the provision of electronic administrative services and, therefore, constitutes a central element in e-Government.

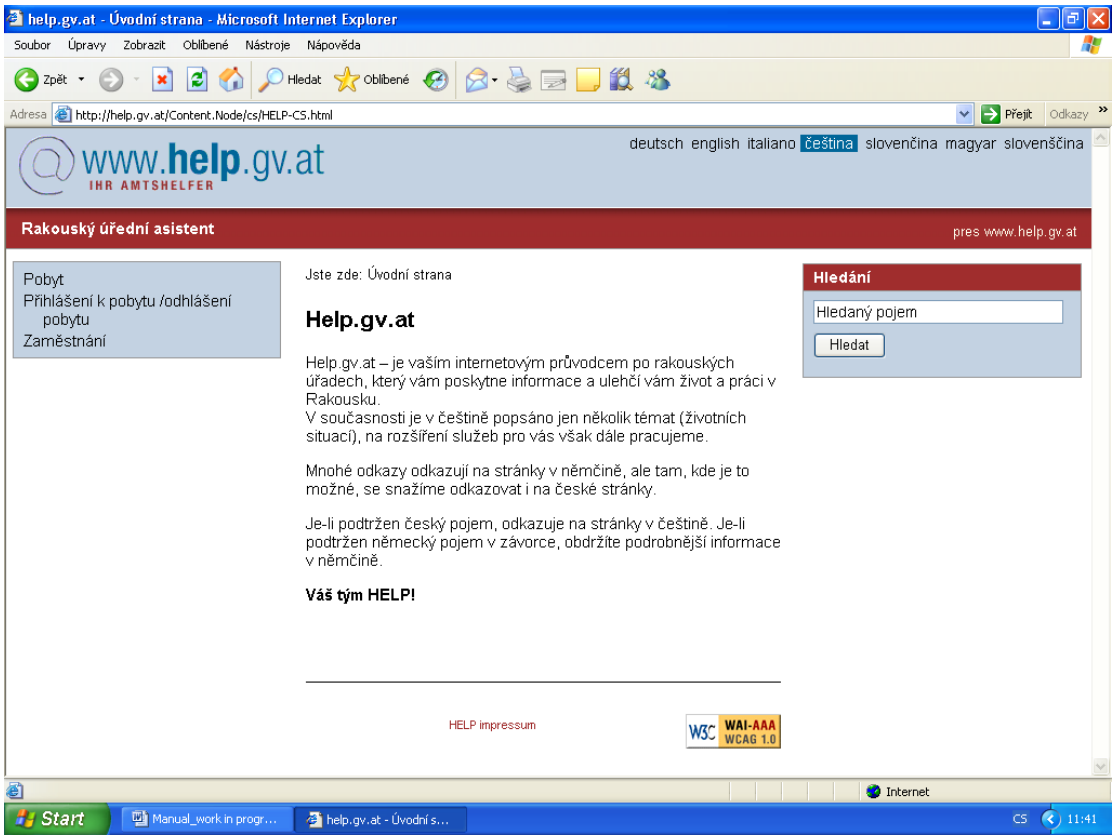
In order to facilitate access to Internet services of the Austrian administration, the existing Austrian administrative portal help.gv.at has been and will further be developed into a transaction portal. It should be possible to obtain all services of public administration through the provided contact point. To use it, the citizens do not have to know individual responsibilities of the authorities. Instead, when seeking information, they can get a better understanding of the provided services based of different circumstances - business and business situations. This should lead to the application of the one-stop-principle of the European Union in the field of e-Government.

The site Help.gv.at is a central instrument to be used to provide administrative procedures in all areas of administration to the public. The use of uniform forms and application processing should help citizens in completing the forms. Within the framework of authorities, the site help.gv.at supports the link between electronic forms and electronic file management or automated procedures, such as "On-line finances".[66] In addition to its barrier-free design, the website help.gv.at is also partially available in the languages of the neighboring countries of Austria. The Czech version can be accessed at: http://help.gv.at/Content.Node/cs/HELP-CS.html:

---

65 *Elsas*, Realisierung eines One-Stop-Government-Portals mit Web Services, in *Wimmer* (Hrsg.), Quo Vadis E-Government: State of the art 2003, 145.

66 https://finanzonline.bmf.gv.at/



In 2006, Austria ranked first during the benchmarking[67] of basic services provided within e-Government which was performed for the 6th time. The study was performed in 28 European countries (25 Member States, as well as Iceland, Norway and Switzerland).

Austria is ranked among the best performers, with 95% for on-line services and 83% for the highest transaction levels, which means that in Austria more than 83% of public services can be provided completely electronically.[68] This result is to a large extent attributable to the promotion of on-line forms mentioned above, as well as their processing using the central administrative portal help.gv.at.

The Czech Republic is placed in the lowest one-third of benchmark results, with only 61% for on-line services and 30% of the highest transaction steps. It seems to have an enormous potential of increase. However, very good basic approach has been shown by Ministerstvo práce a sociálních věcí (Ministry of Labor and Social Affairs) which provides forms for social benefits or social welfare payments both in printable versions and on-line with an electronic signature.[69]

67 http://www.de.capgemini.com/m/de/tl/EU_eGovernment-Studie_2006.pdf

68 The on-line availability of 20 basic services (12 for citizens and 8 for businesses) was evaluated by means of transaction levels.

69 http://forms.mpsv.cz/sspforms/

9.5.5 Back-office and front-office

The terms front-office (external area) and back-office (internal area) are closely linked to the term 'portal'. Electronic communication involves both visible external relations with customers and internal relations which only comprise individual administrative authorities. In the long term, it is not reasonable to promote a single area since media breaks and restructuring processes to a large extent hinder work processes. Rather, internal and external procedures have to be harmonized and, if possible, connected with only a single compatible interface. The communication flow and data flow have to be flowing jointly. In this respect, portals have a duty to interconnect there two areas both from the organization and technical point of view. In doing so, the factual division is bridged in order to establish a continuous system.

However, it may lead to adjustments in regular administrative procedures. Therefore, it is necessary to view the requirements with regard to administration reorganization as a positive step. The task of the adjustment of administrative procedures is also connected with a paradigm change within individual authorities which leads to better service orientation of administration while priority is given to the perception of citizens. The citizens should be provided help with respect to their problems and requests. In this context, specific areas of issues should be formulated by means of the principle of life situations which help to deal with the actual complexity of authority responsibilities. It also leads to an expanded field in which IT tools can be used. The focus is increased and shifted from the actual purely internal IT processes to media-break-free external IT processes. Thus, the clear separation of the terms back-office and front-office get somewhat blurred and by means of mutual integration becomes a key factor for further provision of successful e-Government solutions.[70]

10 An example of gradual implementation in Austria

10.1 What are the changes in administration?

In the past, authorities were characterized by differently organized processes and organizational procedures. An increasing use of information and communication technologies has led to closer cooperation reaching beyond administrative borders. It has led to the promotion of interoperability, transparency, closeness to citizens and customer orientation.

The new approach is based on common service-oriented infrastructures, open interfaces, dynamic applications, modularity and change management. This approach, accompanied by technical and organizational integration of administrative procedures, ensures in the long run a flexible and interactive system of administration. The system of voluntary coordination is replaced by mandatory cooperation between authorities at different levels.

---

70 *Traunmüller/Wimmer*, E-Government at a Decisive Moment: Sketching a Roadmap to Excellence, in: *Traunmüller* (Hrsg.), Electronic Government, 1.

The technological and organizational modifications in public administration bring about considerable changes with respect to staff working in the field. New processes and new software which regularly become available, e.g. electronic act (ELAK), require continuous adaptation of their technical, organizational and social skills. It is therefore necessary that civil servants are further trained in order to ensure that they will be able to deal fast with e-mails, manage requests for information and other matters with which customers approach administration offices. A qualitatively new contact with citizens is also a challenge. Service and customer orientation are of high significance in this respect.

The expectation of a fast and relatively form-free management of matters equivalent to communication in the form of an e-mail leads to significant changes in the work of public services, which also bring about changes in usual decision-making structures (execution capacity) of administration.

In addition, technological progress provides the possibility of teleworking for which it is necessary to establish satisfactory general conditions for all involved.

10.2 Challenges

Recently, electronic services provided by public administration have served in some areas as a pioneer with respect to other authorities. ”Finances on-line“, the on-line government agency help site “help.gv.at”, the legal information system of the Federation (“RIS”), Commercial Register or Land Register are websites, to name just a few, which have been imitated internationally and used as an example.

The EU-initiative eEurope 2002, which was completed in a timely manner as expected, showed as early as in 2000 that the then fragmented IT landscape used in public administration is not suitable for sustainable development of the Austrian e-Government. Loose cooperation between individual administration departments (authorities) in the area of IT had to be replaced by mandatory cooperation.

Politically, news targets were set and incorporated into the Government Program. By 2005, administrative services had to be available for citizens and businesses also in an electronic form.

In parallel to EU work, the reassessment of the federal IT strategy in spring 2000 meant the first steps for the achievement of comprehensive e-Government. From the organization point of view, the new strategic direction manifested itself by means of the establishment of ICT Boards and a Chief Information Officer required by the federal government. To promote the idea, a new administrative department - Federal ICT Strategy - was established whose staff members were to a large extent provided by federal ministries as a token of newly enhanced cooperation.

The ICT Board is a body which was able to develop Federation-wide clear requirements for the establishment of uniform e-Government. At the same time it was clear that e-Government

couldn't be confined within federal, provincial (Länder) or municipal borders. Therefore, it was necessary to establish an open and constructive cooperation with all actors at all levels. It was developed in a transparent manner in agreement with provinces (Länder), municipalities and cities in order to ensure the success of the necessary concept and strategies.

Internationally, the Austrian model is characterized by an integral development approach to e-Government. All its elements and solutions have been implemented Federation-wide in all administrative departments and offices. Applied technical solutions, e.g. security layer, electronic delivery, electronic payment or electronic signature are based on internationally recognized standards and are technologically neutral.

Electronic administration is not only intended for citizens, many e-Government applications are also useful for businesses. For many of them, on-line management of administrative procedures is not a new element since they have already had a chance to make use of IT solutions to establish contacts with authorities in the past. Nevertheless, the introduction of e-Government elements has affected the economy in a particularly significant way. First, it is necessary to ensure adaptation to new technologies. Second, businesses may use the new elements, e.g. Citizen Card or personal identifiers specific for individual industrial sectors, also to perform electronic business transactions with their economic partners or customers and achieve considerable gains in the area of security.

To pave the way for electronic administration it was also necessary to make organizational and legal adjustments. Current legal rules and regulations, which so far covered only traditional "paper administrative processes", have to be extended to cover also electronic administrative procedures. The elements of e-Government, such as Citizen Card, electronic requests, electronic signature, electronic payment and electronic delivery will be made possible through the e-Government Act.

Quality-oriented e-Government requires high-quality infrastructure. New information and communication technologies can only be used if there are high-capacity network accesses available. In order to promote broad-band access, the users could deduct the costs related broad-band access deduct from their taxes in 2004 as special expenses. In addition, Public Internet Access Points (PIAP) provided by means of public terminal in public buildings or by means of WLAN networks should contribute to the measures aimed at infrastructure development.

Today, we live in an ever-changing society. Information and communication technologies surely have a key role to play. To achieve success in life, information and knowledge will be increasingly important in the knowledge-based society. The use of electronic media and technologies in administration requires necessary skills not only from civil servants. Also, citizens have to be able to deal with the newly offered possibilities. A user-friendly uniform design and logical procedures should make the possibilities e-Government has to offer easy to use.

The advances of digital administration and electronic participation offers may not lead to a "society of two classes". At the same time, the expression of opinions should not lead to "transparent" people. This dual challenge requires that the topic of e-Governance is dealt with in especially careful manner. Everybody who wants to use electronic administration should have the possibility; either using his own PC at home or a public terminal. E-Government services as an alternative to traditional visits in an office have to be simple and openly accessible. Help systems should contribute to an easy transfer to the new system and be helpful to the customers in performed individual steps advising them how to do it.

10.3 General conditions

The public expects that the performance of a modern administration will be service-oriented. Therefore, state-of-the-art information and communication technologies have become an inherent part of public administration. New quantitative criteria, such as efficiency, promptness, service orientation, flexibility and security belong to the characteristics which are at present aimed at.

The Internet offers new communication possibilities for internal administrative processes. Whereas, in the past, only some steps of administrative procedures could be performed electronically, at present it is possible to perform complete transactions. A broad implementation of electronic signature guarantees necessary information security and cryptography for the future. The implementation and use of these technologies has to be taken for granted.

Along with technological developments, also the image of administration, as perceived by itself, has changed. The image of fragmented administration has been separated from the One-Stop principle which has been established on the European level. The citizens should not be troubled by the complexity of the administrative system and competence issues any more. It has to be possible to access a service from a central contact point regardless of which processes have to be involved on the part of administration. Thus, the service will become a synonym of straightforwardness, comfort and prompt management.

10.4 Overall concept

Modern and efficient administration is characterized by interoperable system architecture, safe automated business processes, technology-independent development, structured and standardized process models, cost consciousness, integration of existing methods and procedures, network and information security, and change management. The obsolete fragmented structure of administration shall be eliminated by means of a cooperative administrative model.

E-Government in information age leads to a new quality of the relationship between citizens and authorities. New communication possibilities and technologies provide users with a new, free and open access to the virtual world of public institutions. Public administration is ridding

itself of its bureaucratic character and is being changed into an efficient, service-oriented service provider.

In this way, applicants turn into clients. User-friendly procedures, transparent processes, quality-oriented services and closeness to citizens all belong to the main characteristics of modern administration. Administrative procedures provided to citizens and businesses are performed interactively in a dialog, without complications and time loss. Official notifications and documents are provided by authorities in an electronic format. Electronic signature and encrypting mechanisms warrant data security, integrity and protection.

E-Government provides a chance for citizens to be part of opinion-forming and decision-making processes. Public discussion forums and Internet chats may be used to intensify the dialog between citizens and political decision-makers. In the virtual world, it will also be easier to achieve the involvement of citizens at the forefront of legislative processes.

10.5 Objectives

In order to achieve smooth running of automated processes, it is necessary to have a common approach to the concept of the procedures. Current business processes have to be analyzed and remodeled, if necessary.

Close cooperation between authorities at all levels leads not only to improved quality but also to valuable synergies. Sharing of infrastructure, prearranged work and cost sharing when designing processes and coordinated actions related to the development of technical procedural modules help to avoid overlapping and isolated applications.

The new approach to administrative cooperation has been applied to large portions of administration, over and beyond the IT field. In order to make the administrative culture more solid, this approach also has to be taken over by staff members of administrative offices. Therefore, they should have the possibility to get acquainted with new technologies before new administrative procedures are implemented.

In the long-term, we will have to come to terms with new technical concepts. They have to be accepted to a reasonable extent, should the development of e-Government not come to a halt. Therefore, strategic considerations have to be aimed at, from the very beginning, to change management, in order to maintain the future-oriented approach. Especially in the field of security, it is not only innovations we have to face but continuously also additional and higher requirements.

Versatile technologies require continuous education and training of civil servants. Organization and sharing of knowledge is a central element of an efficient modern administration. The future will bring a broader range of applications which enable an active participation in administrative procedures. The qualification of administrative staff members in the field of IT and e-Government has to be increased in order to be prepared to address the challenges; respective e-Government training courses will provided. Outsourcing of operative

duties, as well as an increased involvement in strategy and structure changes, has to be accompanied by a considerable increase of social and technical skills.

10.6 Principles

The Austrian e-Government strategy is based on several important principles:

- Closeness to citizens. Administration has to serve citizens and not vice-versa. On-line services have to be easy to find.

- Comfort through efficiency. When using on-line services, citizens expect a higher comfort: no office visits, no restrictive office hours, no lines, no referrals from one authority to another; instead, uncomplicated procedures, "intelligent forms" which are easy to be filled out, responsible handling of data and prompt management have to be offered. To be able to meet these expectations, the authorities have to optimize their processes by means of automation and modeling.

- Trust and security. Electronic administrative processes have to be as safe as classical channels. In the electronic world, the identification and authentication of persons will be performed through sector-specific personal identifiers and electronic signature. Safe sharing of communication and data transfer will be ensured by established security standards.

- Transparency. Whether technical solutions will be successful and accepted depends on the involvement of all the groups concerned. Initial cooperation between industry and administration is of utmost importance in order to ensure that the implementation is a common issue of all the stakeholders. Transparent processes are essential to such cooperation.

- Accessibility. The services provided by the authorities have to be accessible without discrimination. This is also true for the new electronic administration. E-Government should be available to all classes and groups of population. It is necessary to prevent any technical and social barriers. The acceptance of the Web Accessibility Guidelines[71] should contribute to minimize any risks of exclusion. Widely available public terminals should facilitate the way to e-Government in Austria. At this point all stakeholders - Federation, provinces (Länder) and municipalities - are called to make all possible efforts to achieve this goal.

- Usability. Electronic services have to be designed so as to be provided in a clear and simple manner. A uniform lay-out of forms and portals - classified according to life situations - makes the arrangement more clear, and navigation and usability simpler.

- Data protection. In the eyes of its citizens, Austrian administration is highly trustworthy as far as data protection is concerned. The application of new technologies in administration makes it possible to further develop the trust to cover electronic administrative systems as well. The currently high level of data protection is guaranteed by the use of

[71] Guidelines of the World Wide Web Organization which should ensure non-discriminatory access to information provided on the web, http://www.w3c.org/WAI

electronic signature for authentication of persons and encrypting mechanisms. The instrument of sector-specific personal identifiers developed especially for identification compliant with data protection requirements ensures that within the field of administration only authorized persons are granted access to personal data.

- Cooperation. Smoothly-running e-Government can only be achieved by consistent cooperation at all administrative levels. It is necessary to encourage the sharing of available applications and infrastructures in order to guarantee the efficiency strived for with regard to organizational, financial and administrative aspects. Cooperation between individual authorities is based on the fundamental idea of making interfaces openly available and providing basic functions free of charge.

- Sustainability. The modular structure facilitated change management which enables continuous development in the field. Open e-Government contributes to improved competitiveness and thus to safeguarding of Austrian economic position. A significant role is played by strategic coordination of the IT field within administration.

- Interoperability. The systems have to communicate with each other. Therefore, implementation-oriented e-Government conventions based on internationally recognized standards and open interfaces are designed.

- Technological independency. The development of information and communication technologies is rather fast-paced. Therefore, e-Government solutions have to be open to any new technologies. It is not possible to prefer any specific technologies. It is necessary to eliminate any dependency on monopoly positions.

The application of information and communication technologies makes it possible to organize public administration according to these principles. The provision of electronic services is an alternative to traditional administrative channels which is available around the clock. Citizens are free to decide which one of these alternatives they wish to use. The risks of digital exclusion are tackled by open e-Government which is available to all groups of the society.

10.7 Cooperation processes

10.7.1 National cooperation

Since the activities of the ICT Board were launched, emphasis has been placed on cooperation between the Federation, provinces (Länder), cities and municipalities. The principle of transparency is implemented through the publication of its decisions on the website www.cio.gv.at.

The reference server established by provinces serves as a communication platform used to publish internal work concepts, draft concepts, discussion items, intermediate results for interested business, but also conventions agreed by the Federation and provinces.

To a large extent, administrative activities are performed by provinces (regional administrative authorities), cities (municipal administrative authorities) and communities. Without coordinated work on basic principles, a strongly federalized structure of the Austrian system of administration would in the long run lead to varying methods and approaches. Citizens and businesses would have little understanding for such a situation. Therefore, a common coordinated approach is a principle leading to the beneficial implementation of e-Government.

In order to be able to make use of these synergy effects, IT activities at the provincial and federal levels are coordinated in different work groups setting common priorities. In agreement with the ICT Board, demand-oriented work groups are established in order to promote coordinating activities. This leads to deciding about concepts and projects before any field-specific or comprehensive decisions are taken. In such a way, it is possible do prevent any divergent views at a professional level.

10.7.2 International cooperation

As mentioned above, one of the main parts of the e-Government strategy is to create and disseminate interoperable solutions which make Austrian approaches comparable internationally. Austrian concepts will be presented both at the EU level and at different international forums. Identity management and interoperability, as well as such fields as recognition of electronic documents and long-term archiving are the priorities which will be increasingly focused on in the EU agenda during the Austrian EU presidency in 2006. In addition, an Austrian initiative launched in 2003 which is aimed at establishing a "virtual e-Government Resource Network" will be further developed during the Austrian presidency.

10.8 Basic legal principles

10.8.1 E-Government Act

The e-Government Act[72] took effect on 1 March 2004. It provides a legal basis for implemented e-Government instruments and the possibility of closer cooperation of all official e-Government providers. New instruments such as Citizen Card, sector-specific personal identifiers or electronic delivery may also be used by economic actors.

The highest principles comprise:

Free choice of communication to be used for delivering applications to authorities.

Security to improve legal protection through the implementation of technical measures, e.g. Citizen Card.

72 Federal Code I No 10/2004

Barrier-free access for people with disabilities to information and services provided by public administration by 2007 by means of the compliance with international standards governing accessibility of the Internet.

The most important requirements can be summarized as follows:

Citizen Card

By means of a Citizen Card, persons approaching any authorities may be unambiguously identified and any documents exchanged during the communication authenticated. Applications can be assigned to individual persons and these persons can be provided access to their personal data without running a risk with respect to data protection. To be sure that an application is authentic and has not been falsified ex-post, it has to be possible to authenticate any application. It is possible to perform the identity and authenticity check using the Citizen Card and electronic signature while complying with any data protection requirements. The Citizen Card may also be used for e-Commerce to achieve increased technical and legal security of Internet transactions. It is a technology-independent tool. It is not important which technology has been used as a supporting medium, whether a chip card, cell phone or any other technology. Vital is that a Citizen Card can link an electronic signature to a certain person, relevant security data and functions, as well as any data about a power-of-attorney, if applicable.

Personal linkage

The principle of personal linkage ensures a clear link between a Citizen Card and a legitimate owner of the card. To be more specific, the "Stammzahl" Register Office confirms, by means of electronic signature, that the owner of the card has been assigned a unique identification code (a so-called "Stammzahl" or a *stem code*) to ensure unambiguous identification. Information about this personal linkage will be saved to the Citizen Card.

Power of attorney

It is possible to authorize a different person to file applications on one's behalf. In this case, the "Stammzahl" Register Office will use the Citizen Card of the authorized person to save the "Stammzahl" of the authorizing person and the existence of this relationship between the two persons, including any possible time or substantive limits. Powers-of-attorney may also be obtained for legal representative.

Unique identification code ("Stammzahl")

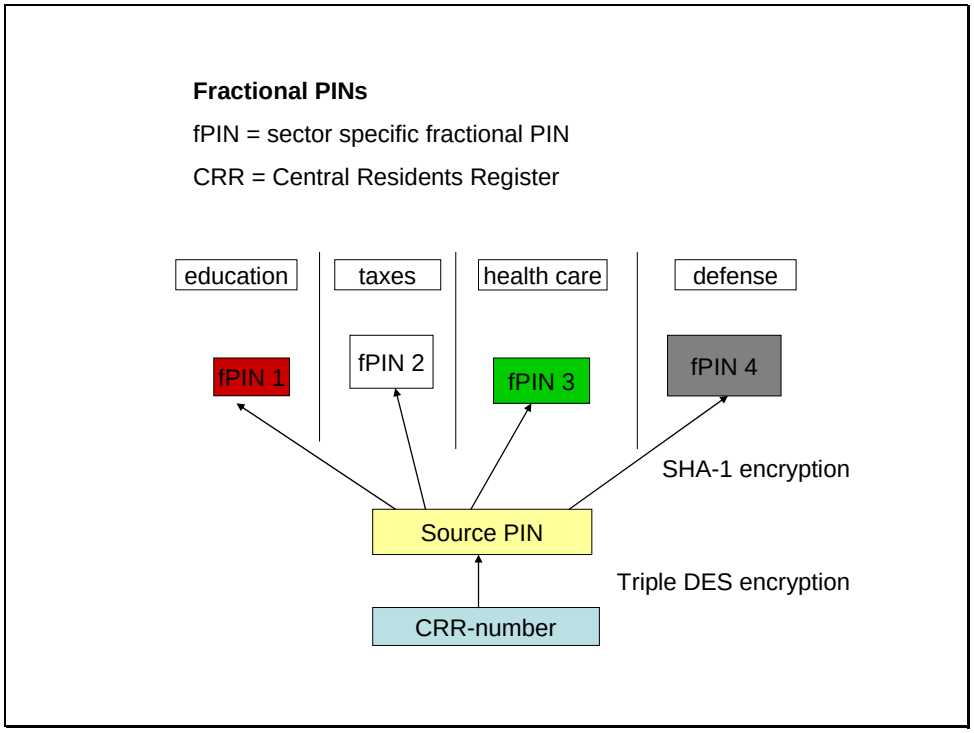
Each natural person permanently resident in Austria will be assigned a unique identification code for unambiguous identification, a so-called "Stammzahl", which is strongly encrypted and derived from the personal identity code of the CRR (Central Register of Residence, "ZMR-Zahl"[73]). For all other natural persons, a serial number is used from the Supplement

73 A unique personal identification code of the citizen based on the Central Register of Residence

Register in order to be able to generate the "Stammzahl". The "Stammzahl" of a natural person may only be saved on Citizen Cards. For legal persons, their Commercial Register number, Central Associations Register number or a serial number used in the Supplement Register are used to generate the "Stammzahl" (see the Graph under the section "Register of stem codes").

Sector-specific personal identifiers

In order to provide data protection, the *stem codes* of natural persons may not be saved by authorities. Natural persons may only be identified by authorities using sector-specific personal identifiers. These are generated from the „Stammzahl" of the person in question. Their generation may not be traceable or reversible. A sector-specific personal identifier is valid only for the scope of actions performed by the authority in question which is responsible for any particular procedure. To detect a sector-specific personal identifier, the "Stammzahl" of the person concerned is necessary. The "Stammzahl" may only be used for the generation of the sector-specific personal identifier under cooperation of the person concerned, i.e. using of his/her Citizen Card. If the "Stammzahl" is unknown, the sector-specific personal identifier may be generated without the Citizen Card of the person concerned only by the "Stammzahl" Register Office under certain circumstances.

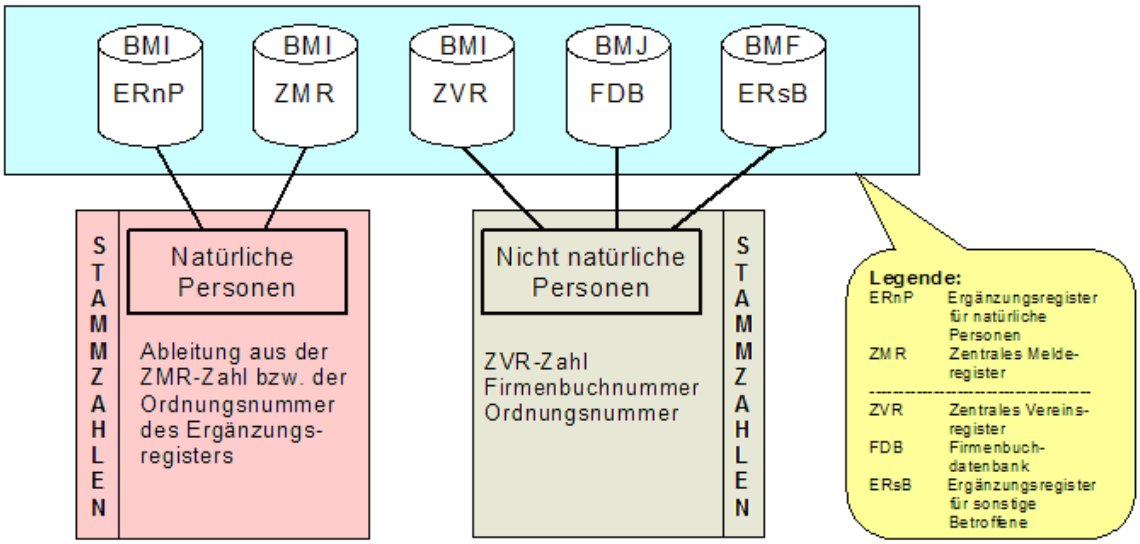


"Stammzahl" register

The „Stammzahl" Register is used to obtain *stem codes* which are used for unambiguous identification of persons. The Stammzahl" Register Office is a data protection committee

(Zentrales Melderegister).

which serves the Federal Ministry of the Interior (Bundesministerium für Inneres - BMI) and the Federal Ministry of Justice (Bundesministerium für Justiz - BMJ).



Supplement Register

All individuals with no official residence in Austria or legal persons, if applicable, which are not registered in the Commercial Register or the Central Associations Register, may be registered in the Supplement Register if they want to establish an electronic contact with authorities.

Administrative signature

Until the end of 2007, administrative signature shall be treated in the field of public administration as equal to a secure signature within the framework of Citizen Card function which means that it can be used for all official procedures instead of a secure signature. Administrative signatures are signatures which provide sufficient security with respect to identity and authenticity verification, however, they do not necessarily meet all the requirements concerning a secure signature; in particular, they are not necessarily based on a qualified certificate. Security and organizational prerequisites with regard to administrative signatures are stipulated in the Administrative Signature Regulation (Federal Code II No 159/2004).

Standard document register

So far, in order to initiate a certain procedure, citizens and businesses had to repeatedly provide evidence to document certain data by means of such documents as birth certificates, proof of citizenship or excerpts from the Commercial Register. In the case of electronic administration, it can be in many cases avoided because it is possible to use the existing electronic data available from the registers. For this purpose, the accuracy of the available data

related to the person's status and citizenship is checked during registration procedure by the relevant authority by means of verification of any relevant documents (standard documents) and such information is provided to the Central Register of Residence. Natural persons may also ask for certification of accuracy of their data outside the scope of registration procedure, if they document the accuracy of their data by means of relevant documents to the registry office. Thus, certain data does not have to be provided repeatedly; rather, it can be asked directly from the Central Register of Residence with the consent of the person in question. Alternatively, the applicant may also submit an electronically signed Registration Certificate of the Central Register of Residence. Businesses may use the Document Register in accordance with Article 114(2) of the BAO[74] in order to provide electronic evidence of their authorization to exercise their profession or the type of the activities they perform.

Official signature

Administration staff members have to be sure that electronic documents received from authorities are authentic. An official signature is an electronic signature which is appended by an authority to an official notification or a document. It makes electronic documents easily identifiable. Official signature serves not only to check the authenticity of a document. In addition, for printed documents, it has an effect of authentication if the document can be transformed back to its electronic form.

Electronic delivery

Documents from court and administrative bodies can be provided electronically through a delivery service. Citizens and businesses wishing electronic delivery can register with a delivery service by means of their Citizen Card (signature card or cell phone). After that, they can receive documents from authorities through the delivery service. In such a case, the delivery service notifies the person in question that a document is ready to be sent electronically. In order to protect the documents from access of a third party, the delivered document can only be retrieved upon identification and authentication by means of the Citizen Card. In addition, it can only be delivered in an encrypted form which can only be decoded (decrypted) by the owner having access to the Private Key. To start operating the delivery system, the delivery of the first communication (notification) to the addressee of the document is decisive. Legal effects of delivery occur upon the collection of a document, however, not later than one week of the day of sending the first communication (notification). The electronic signature generated by the addressee at collection serves as evidence of delivery for the authority in question. Delivery services may only be offered by private entities. As long as all stipulated conditions have been fulfilled, the authorization to provide delivery services is made through a notification.

74 Federal Fiscal Code

10.8.2 The "Stammzahl" Register Regulation

- The "Stammzahl" Register Regulation took effect on 3 March 2005 (its fourth paragraph on 1 July 2005).[75] The Regulation governs the activities of the "Stammzahl" Registration Office and its cooperation with its service providers necessary for the implementation of the Citizen Card concept. The following are the essential provisions of the Regulation concerning:

  - The procedure governing the **creation of personal linkage**, especially the responsibilities of the Citizen Card Registration Office, identity authentication and personal linkage dataset. It is also regulated that the environment suitable for dealing with Citizen Cards means only the interface defined by the "Stammzahl" Registration Office as suitable for linking a Citizen Card to a specific use of data of a client. The description of the interface is to be published by the Stammzahl" Registration Office.

  - Legal definition of **repeated identity check**. Repeated identity check is designed for persons with an electronic signature but no personal linkage who still want to communicate with authorities electronically in accordance with the procedures of the e-Government Act. In particular, it is meant for persons who live abroad and consequently do not have an offhand possibility to acquire a Citizen Card. It means that also foreign electronic proofs of identity can be integrated into the Austrian e-Government system. Repeated identity check enables to identify electronic identity without personal linkage within the environment commonly using Citizen Cards.

  - Conversion of sector-specific personal identifiers into foreign sector-specific personal identifiers, **calculation of sector-specific personal identifiers** for certain cases of power-of-attorney and the equipment of data applications of the client of the public sector. For the calculation and conversion of sector-specific personal identifiers, the "Stammzahl" Registration Office makes a special service available to authorities in the form of an interface, which is also possible to reach through the portals of specific authorities. Each application for the calculation of a sector-specific personal identifier has to be recorded by the "Stammzahl" Registration Office.

    - Example:

    - A school is delivered a request, within the field of "Education and Research", concerning the social security of one of its students (field "Social security") - see the Graph showing individual steps below.

---

75 Federal Code I. II No 57/2005

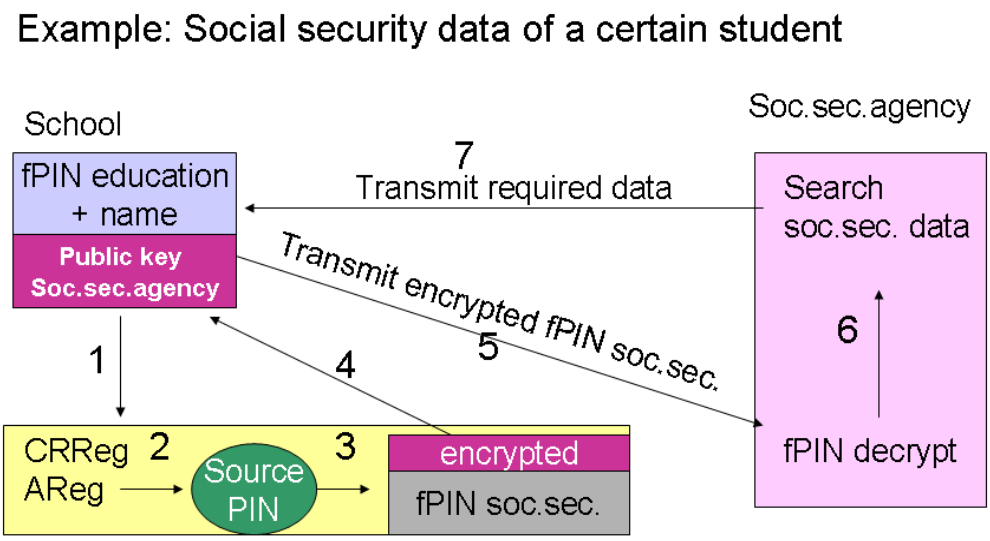
The school communicates the request (1) to the “Stammzahl” Registration Office: its own sector-specific personal identifier “Education and Research” along with the name of the student and a public key of social security to which the data should be transferred.

It is necessary to provide the name of the student because sector-specific personal identifiers are not reversible due to the hashed code procedure used and, therefore, it is not possible to calculate the “Stammzahl” of the person in question just knowing his/her sector-specific personal identifier. At this point (2), the “Stammzahl” Registration Office calculates all the *stem codes* and sector-specific personal identifiers in the field “Education and Research” of the persons having the same name as the person in question and compares them with the communicated sector-specific personal identifier of that person in the field “Education and Research”. It requires the cooperation of both the Central Register of Residence and the Supplement Register. By means of comparing these numbers, the “Stammzahl” Registration Office finds an identical sector-specific personal identifier.

It enables the Office to calculate the sector-specific personal identifier of the person in question in the field “Social Security” using his/her *stem code* (3).

The sector-specific personal identifier in the field “Social security” will be encrypted using the public key social of the security system to which the data should be provided (4). The encrypted sector-specific personal identifier “Social security” will be provided to the school which delivers to social security the data to be communicated along with the encrypted sector-specific personal identifier “Social security” (5).

Social security receives the data and decrypts the sector-specific personal identifier, encrypted by its own public key, using its private key receiving thus the required sector-specific personal identifier “Social security” (6). Using the received sector-specific personal identifier, social security can now find the social security information about the insured person in its databank and provide the requested data (7). This procedure should be used as described, although it has not been provided here for clarity consideration.



- Electronic provision and verifiability of **powers-of-attorney** within the Citizen Card concept. The possibility to electronically see whether a person has provided its power-of-attorney to somebody else in the Citizen Card is one of special achievements of the Austrian Citizen Card concept. The "Stammzahl" Registration Office signs the proxy dataset making any unnoticed falsification of these records on the Citizen Card impossible. The "Stammzahl" Registration Office will also set up an Internet address to provide a possibility of cancelling such powers-of-attorney on-line.

10.8.3 Regulation specifying the area of E-Government

In order to calculate-specific personal identifiers, each use of data of a public sector client has to be attributed to a specific state field of activity. The Regulation specifying the area of E-Government[76] stipulates the description of each field of activity, including field-specific abbreviation.

At present, we distinguish between the following fields:

Activity sector	**Sector-specific abbreviation**	**Examples**
Work	AR	*Employee protection,* *Labor market management*
Official statistic	AS	
Education and research	BF	*Schools,* *Universities,* *Vocational schools,* *Other educational and research establishments,*

[76] Federal Code II No 289/2004

Activity sector	Sector-specific abbreviation	Examples
		Scholarships, *Validation,* *Libraries and archive*
Construction and living	BW	*Construction procedures,* *Housing redevelopment,* *Municipal housing,* *Arbitration according to the Tenancy Law,* *Housing support,* *Promotion of energy saving,* *Channel interface,* *Urban and regional planning, road traffic, water supply*
EU and foreign affairs	EA	*Consular services,* *Austrians living abroad*
Import / Export	EF	*Import and export licenses,* *Customs*
Health care	GH	*Nursing, health care,* *Health care education,* *Vaccination,* *Monitoring of poison handing,* *Monitoring of communicable diseases,* *Monitoring of fight against drug abuse,* *Undertaking*
Society and social affairs	GS	*Support of individual social groups, e.g. ethnic groups, women, families, people with disabilities, generations, consumer protection, child care establishments, general care,* *social emergency services, social care (excepting medical care),* *Management of non-profit foundations*
Restitution	GS-RE	*Restitution affairs*
Justice/Civil law	JR	*Civil jurisdiction,* *Execution,* *Notarial and attorney affairs, including defense lawyer in criminal cases,* *Land Register,* *Commercial Register*
Religious affairs	KL	*Churches,* *Religious societies*
Art and culture	KU	*Culture support,* *Preservation of monuments*
Agriculture and forestry	LF	*Agricultural subsidies,* *Animal husbandry and livestock breeding,* *Hunting and fisheries*
National defense	LV	*Military services,* *Military fees,* *Mobilization,* *Alternative civilian service*
Radio and other media, as	RT	*Radio fee,*

Activity sector	Sector-specific abbreviation	Examples
well as telecommunications		*Media support,* *Telecom regulator,* *Supervision of the Signature Act*
Taxes and levies	SA	*Taxes, fees (e.g. for communal supply services)*
Sport and leisure	SF	
Safety and order	SO	*Security police,* *Firearms law,* *Right of organization,* *Lost-and-found service,* *Emergency management,* *Crisis management,* *Rich of assembly and right of association*
Associations Register	SO-VR	
Criminal Record	SR-RG	
Social security	SV	*Unemployment insurance,* *Health care insurance,* *Accident insurance,* *Retirement pension insurance*
Environment	UW	*Water laws,* *Waste managements,* *Air pollution control,* *Nature and landscape protection*
Transport and Technology	VT	*Traffic police,* *Motor vehicles agenda,* *Driving licenses,* *Technical services*
Asset management	VV	*Asset management of clients,* *Acquisition, procurement,* *Office management,* *Vehicle fleet*
Economy	WT	*Trade,* *Apprentice and master examinations,* *Tourism,* *Industry,* *Energy industry*
Personal identity and civil liberties (of a person)	ZP	*Citizenship,* *Marital status,* *Withdrawal from religion,* *Registration of residence,* *Alien affairs,* *Passports,* *Elections*

If cross-sectoral data application is necessary in the case of a public sector client, especially if central services are provided, they can be provided cross-sectoral identification (abbreviation) which, at present, are the following:

Activity sector	Sector-specific abbreviation	Examples
Trans-sectoral legal protection	BR	*Court under public law,* *general supervision, e.g. Neighborhood watch,* *Supervisory activities, e.g. Court of auditors,* *Advocacy*
Central accountancy	HR	*Central clearing point for e.g. fees and administrative fees,* *but also for private services provided for or by clients*
Internal general record keeping of clients	KI	*Trans-sectoral electronic file management systems*
Public relations	OI	*Citizens' affairs,* *Presentation of clients in the media,* *Call center*
Personnel administration	PV	
Central legal service	RD	
Central management of administrative criminal proceedings	VS	
Central administrative criminal records	VS-RG	
Deliveries	ZU	

10.8.4 Regulation on Supplement Register

Along with the "Stammzahl" Register Regulation and the Regulation specifying the area of E-Government, the Regulation on Supplement Register[77] forms one of the principal implementation regulations to the e-Government Act. The Regulation is an important contribution to the implementation of the Citizen Card concept because it enables to unambiguously identify natural and other persons in questions which, for various reasons, may not be entered into the basic register of e-Government. Consequently, the Supplement Register was established for natural persons in addition to the Central Register of Residence. All other persons are entered into the Supplement Register to the Commercial Register or to the Central Associations Register. Therefore, the Supplement Register is maintained in two parts, separately for natural persons and for "other persons". In accordance with the e-Government Act, the part of the Supplement Register set up for natural persons is the responsibility of the Federal Ministry of the Interior, which is considered to be a service provider, whereas the other part is the responsibility of the Federal Ministry of Finance.

77 Federal Code II No 241/2005

10.8.5 Regulation on Administrative Signature

First and foremost, the Regulation[78] is meant for the providers of administrative signatures and Citizen Card governing necessary security and organizational requirements for signature creation. Compliance with the Regulation is ensured by means of the cooperation of the "Stammzahl" Registration Office necessary for issuing Citizen Cards. The "Stammzahl" Registration Office may only support Citizen Card by means of administrative signatures when the type of the administrative signature meets specified requirements.

Administrative signature is an electronic signature of a citizen which basically meets the requirements of a safe signature, however, is not necessary based on a qualified certificate. In principle, there are two types of administrative signatures: a signature with a signature token (e.g. a chipcard) owned by the user and a server-based signature. On the one hand, the Regulation on Administrative Signature ensures adequate protection of a private signature key, on the other hand, it makes its release dependent on the owner and its knowledge.

For a server-based signature, the data on signature creation have to be available only to the signatory. It is ensured by single-use code used in addition to the authorization code. The single-use code is only available to the signatory. It can´t be systematically communicated by either the security server or any other person. Authorization codes, as well as single-use codes should by adequately protected by encryption when transported by the user to a safe area.

10.8.6 Regulation on Delivery Services

The Delivery Service Act[79] was amended at the same time as the e-Government Act[80] was passed. Electronic delivery is governed by Section III of the Delivery Act which, first and foremost, stipulates the duties and approval of electronic services, more detailed conditions of service provision and supervision over electronic delivery services. In particular, the Regulation on delivery services[81] stipulates precise criteria for approval, which are referred to in Article 29 of the Delivery Act and according to which it is possible to evaluate necessary technical and service capability, as well as legal reliability of electronic delivery services, especially with regard to data protection, with respect to the due provision of the services they are to provide. Necessary technical specifications which are to be met by those interested in delivery service provision shall be defined separately in an Annex to the Regulation and published on the Internet.[82]

10.8.7 Regulation on Delivery Forms

The Regulation on Delivery Forms of 1982 was amended by the Regulation no 235/2004 of the Federal Code 1 II and No 261/2006 of the Federal Code 1 II and added forms to be used

78 Federal Code II No 159/2004

79 Federal Code No 200/1982, as amended by Federal Code I No 10/2004

80 Federal Code I No 10/2004

81 Federal Code II No 233/2005

82 http://www.bka.gv.at/zustelldienste

for individual process steps of electronic delivery. The Regulation lays down the forms for the first, second and third notification, of which the thirds one is not electronic.

10.9 Register

Decentralized and federal organizational structure and responsibilities require a high level of coordination to avoid unnecessary overlapping. The aim is to achieve optimum use of the recourses earmarked for e-Government. The registers used for the provision of e-Government services will be available to all administrative levels by means of a portal network. Thus, authentic data stored in the registers can be used without storing data repeatedly in several systems.

A uniform access to the registers can offer ever more: Commercial Register, Land Register, Associations Register etc. make the procedures for business easier. By introducing electronic signature, the use of open systems which have an independent design and operation will be possible.

Storage of data in central registers is also related to potential risks fort the private sphere of those whose data is stored. Therefore, it is necessary to exercise caution when accessing data ensuring that only the data required by the addressee, which he/she is authorized to receive, are accessed.

10.9.1 Standard Document Register

When dealing with authorities, citizens are repeatedly asked to submit different documents, such as birth certificates or proof of citizenship. By means of establishing the Central Register of Residence (Zentrales Melderegister - ZMR), an infrastructure was created which enables high-quality electronic identification of persons. In the medium and long term, it means that standard paper documents will be replaced. The Central Register of Residence thus becomes a key tool for e-Government:

- The introduction of the Standard Document Register enables electronic provision of certificates. Documents to document personal situation and citizenship data don't have to be submitted physically during a procedure; rather, they can be requested from the Central Register of Residence to be supplied electronically. Practically, the person in question may ask the authorities to check the required data electronically in the Standard Document Register. This shall lead to simplification of administrative procedures.

- It is not necessary to set up one's own register. In the Central Register of Residence, an electronic record will be made to document that residence data is accurate, after the data has been checked for accuracy in local registry offices by means of consulting original documents. This procedure does not mean any additional effort since checking identity data by means of consulting original documents is a requirement. The accuracy of data is then recorded in the Central

Register of Residence directly by local registry offices. Upon the request of the person in question, the accuracy of a registration date may also be recorded by a registry office outside the scope of a regular registering procedure in the Central Register of Residence in the cases when the person submits the necessary document to prove the accuracy of the data.

Alternatively, in addition to a request by authorities, standard documents can also be replaced by a Registration Certificate bearing proof of accuracy of the registration date. A registration Certificate is available both in hard and electronic copies. Similarly to its paper counterpart, an electronic Registration Certificate has an authenticity of an official document because it is electronically signed by the authorities.

If required by the person in question, it is possible to use all electronically available datasets of public institutions as proof of standard documents.

10.9.2 "Stammzahl" register

The "Stammzahl" Register of natural persons is a virtual register. The entries are only made when necessary for the purpose of calculating a *stem code* or a sector-specific personal identifier. After that, they are immediately erased. The "Stammzahl" of a natural person may only be saved to Citizen Cards.

The **"Stammzahl" Registration Office** is a **data protection committee** since electronic identification of persons is subject to data protection regulations. As a service provider it is under the responsibility of the Federal Ministry of the Interior which maintains also the Central Register of Residence. The **"Stammzahl" Registration Office** has the following responsibilities:

- Maintenance of the "Stammzahl" Register;
- Maintenance of the Supplement Register.
- Conclusion of service contract with certification-service-providers in order to facilitate the establishment of Citizen Card registration offices.
- Laying down mathematical procedures necessary to calculate *stem codes* or substitute *stem codes* and sector-specific personal identifiers and their publication on the Internet.

For legal persons, the Commercial Register number, the number from the Central Associations Register or the number from the Supplement Register shall be used as a *stem code*. There registers are established on a continuing basis.

The persons who wish to contract the authorities electronically but have not been entered into any Austrian register (which means they have not even been registered in the Supplement Register, see below), may be identified by means of a repeated identity check. In this case, the

person is not identified unambiguously; however, it can easily be checked that the person is the same as the one who has already been in contract with any particular authority. Upon request, the person in question is provided with a substitute *stem code* which is composed of his/her data (e.g. name, date of birth, place of birth, serial number of certificate, etc.) and provides adequate certainty with regard to his/her identity differentiating him/her from others. It has to be clearly indicates that it is a substitute *stem code*.

10.9.3 Supplement register

During electronic procedures performed by public administration, the "Stammzahl" is used as a basis for the identification of natural person and for the generation of sector-specific personal identifiers. The „Stammzahl" of natural persons is derived from a so-called "ZMR-Zahl" (personal identity code of the Central Register of Residence) which has been unambiguously assigned to the person in the Central Register of Residence. For legal persons, the Commercial Code number of the number from the Central Associations Register is used as a basis for the calculation of their *stem codes*.

Only persons registered in Austria are entered into the Central Register of Residence. In order to provide access to electronic administration by means of a Citizen Card also to the persons who do not have to be registered (e.g. Austrians living abroad), a so-called "Supplement Register for Natural Persons" has been established.

There are also legal persons who are not registered either in the Commercial Register or in the Associations Register, e.g. churches, communities and consortia. These persons also have to have a possibility to participate in e-Government by means of an unambiguous number.

It is possible to use the data entered into the Supplement Register to calculate their *stem code*:

- Persons are registered who have not been registered in the Central Register of Residence, Commercial Register or Associations Register.
- Registration is made upon the request of the person or, in certain cases, upon the request of the client whose data shall be used. In order to make the registration, the person has to submit his/her identity data which is required in accordance with the Registration Act. Non-natural persons have to provide evidence of their legal status and legally effective designation.
- The purpose of registration is to provide electronic proof of the unambiguous identity of the person in question.
- Natural persons and non-natural persons are registered separately. As a service provider, the "Stammzahl" Register Office uses the services of the Federal Ministry of the Interior (for the part "Supplement Register for Natural Persons") and of the Federal Ministry of Finance (for the part "Supplement Register of

Other Persons"). For the latter, also powers-of-attorney and geographic and organizational division (e.g. branches) may be registered.

10.9.4 Central Register of Residence

The operator of the use of data is the Federal Ministry of the Interior. Registry offices are clients from the data protection point of view. The Central Register of Residence is maintained as an information network system according to the Data Protection Act of 2000.[83] The Central Register of Residence is a public register. Information is provided upon proving legitimate interest and submitting certain data.

The total dataset of each person registered in the Central Register of Residence consists of the following elements:

- Identity data
  Name, sex, birth data (place, date, province [Bundesland] if born in the country, and state if born abroad), a so-called ZMR-Zahl (number provided by the Central Register of Residence), and citizenship. For foreigners, the type, number, issuing authority and issue date, as well as the state in which the passport was issued are required in addition.

- Residence data
  Street/house number/staircase/apartment, zip-code, municipality/province [Bundesland] when registering or deregistering, name of housing provider.

During electronic administrative transactions between citizens and authorities, natural persons are identified by means of sector-specific personal identifiers. The "Stammzahl" derived from the so-called "ZMR-Zahl" (provided by the Central Register of Residence) serves as a basis for the calculation of sector-specific personal identifiers. The "ZMR-Zahl" is assigned to each person who has to register in Austria with the Central Register of Residence as a distinctive identification.

In order to adjust to the new functions of the Central Register of Residence within e-Government, the e-Government Act envisages an amendment to the Registration Act:

- The "ZMR" numbers have to be available to the "Stammzahl" Register Office so that it can fulfill its duties.

- If technically possible, requests for information about registration in the Central Register of Residence can be submitted and provided by means of a Citizen Card.

- In order to receive information about a person's principal residence, the interested party has to know the name, family name and one other characteristic element of

[83] Federal Act on the Protection of Personal Data (Data Protection Act 2000 - DSG 2000), Federal Code I No 165/1999

the person. If the sector-specific personal identifier is provided, the requesting party has to submit its own *stem code* to make the examination of the -specific personal identifier possible.

- It is necessary that local authorities, associations of local authorities, court commissioners, and social security providers are allowed to make requests if they are made within the framework of their legally assigned duties.

In order to be able to update the data in the Central Register of Residence, the Register Act was amended within the e-Government Act to that effect that the Central Register of Residence is provided with both updated information with regard to citizenship of persons who are registered in the Austrian Federation and updated information with regard to the name or sex.

10.9.5 Central Associations Register

The Central Associations Register (ZVR) plays an important role in e-Government. The involvement of the Central Associations Register is possible in accordance with the e-Government Act which contains an amendment to the Associations Act of 2002.[84] Similarly to the Central Register of Residence, Commercial Register or Supplement Register, it provides a so-called "ZVR-Zahl" which is an important element for electronic communication between citizens and the authorities. Having been implemented into the portal network system, it facilitates the transactions between individual authorities which are made more efficient due to the use of already available resources.

The Central Associations Register is operated and maintained by the Federal Ministry of the Interior as an information network system. In accordance with the Data Protection Act, the clients of the Central Associations Register are associations' authorities of first instance which maintain, in their local Associations Registers, certain data related to the associations (name, "ZVR-Zahl", data of association, registered office, authorized representatives, and their sector-specific personal identifiers, etc.) resident in the area they are responsible for. The data from local Associations Registers are transferred to the Central Associations Registers using of the information network. In order to provide unambiguous identification of each association, the Central Associations Register assigns it a so-called "ZVR-Zahl" which is provided to the local associations' authority.

The data related to an association are processed in the Central Associations Register in such a way that it may only be accessed on the basis of the name and "ZVR-Zahl" of the association. If there is no information ban, certain data is available on-line for anybody free of charge. Data protection requirements (authorization to receive information, introduction training

84 Associations Act 2002 - VerG, Federal Code1. I No 66/2002

provided for staff members, technical protective measures to hinder unauthorized access, data migration) are stipulated in a Regulation.[85]

11 Identification of persons in electronic communication

From the complexity of an administrative procedure, comprising request for information, internal processing, including Register inquiries and entries, up to delivery of results, it is clear that in addition to a safe electronic access to administration also an unambiguous identification of clients is necessary in order to ensure that data is assessed and handled only by authorized persons. The identification procedure should be uniform throughout the entire administration to make it easier for citizens. Assignment of rights or duties with regard to a certain citizen or a business also requires a clear identification on the part of administration. On the other hand, the basic right to data protection should always be complied with during the procedures.

In electronic transactions, it is important to keep in mind that in addition to client identification it is also necessary to make sure that the provided data is authentic. This aspect is particularly important if we realize how easy it is to manipulate unprotected electronic data especially during its transfer in open networks.

The solution has been provided by the concept of a so-called Citizen Card applied in Austria which combines the advantages of an electronic signature with the allocation of the owner of the Citizen Card to a non-ambiguous state register of persons (Central Register of Residence), thus providing not only the possibility of authentication and identification but also an unambiguous identification.

11.1 Electronic Signatures

11.1.1 Basic legal principles

The main principle to be discussed is the Directive No. 1999/93/EC of the European Parliament and Council of 13 December 1999 on a Community framework for electronic signatures (Signature Regulation). This Directive has also been transposed into the Czech national law. [86]

---

85 Regulation of the Federal Ministry of the Interior on the use of data related to associations for the establishment and operation of the Central Associations Register (Regulation on Associations Data Protection - VereinsDS-VO), Federal Code II No 443/2003

86 Czech Republic: Act No 227/2000 Coll., Zákon o elektronickém podpisu a o změně některých dalších zákonů (Act on Electronic Signature and on the Amendment of Some Other Acts)
Germany: Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Federal Code I 2001, S. 876, as amended by the Federal Code l. I 2005, S. 1970, 2013 (Act on Basic Conditions for Electronic Signatures and on the Amendment of Some Other Acts)
Austria: Bundesgesetz über elektronische Signaturen (Federal Act on Electronic Signatures), Federal Code l. I No 190/1999, as amended by the Federal Code I No 164/2005 (Signature Act – SigG).
Die Verordnung des Bundeskanzlers über elektronische Signaturen (Decree of the Federal Chancellor on Electronic Signatures), Federal Code l. II No 30/2000, as amended by the Federal Code. II

The Directive stipulates general legal conditions for electronic signatures and certain certification services. It provides for a supervision system to supervise certification-service-providers. From technical point of view, the Directive provides more detailed rules only with regard to system functioning; otherwise it is "technologically" neutral in order to comprise any possible technical innovations and improvements within its scope. The definition of the terms used in the Directive is, therefore, rather wide.

In other words, the Austrian Signature Act governs the creation and use of electronic signatures, as well as the provision of signature and certification services.

With regard to legal effects of advanced electronic signatures[87], Article 5 of the Signature Directive stipulates that they shall

- satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
- are admissible as evidence in legal proceedings.

Before the introduction of electronic signatures, communication through the Internet, both by means of e-mails and by sending completed on-line forms, was characterized by uncertainty about the true identity of the communication partner and doubts about whether the communicated data is authentic and has not been manipulated during transfer.

However, business dealing or communication with authorities requires clear information about person's identity and data authenticity beyond any doubt. In usual paper communication, this function is fulfilled by hand-written signature. Hand-written signature serves as evidence of identity of the signatory; it distinguishes the person issuing the document because a distinctive signature provides an unambiguous link between the document and the person signing it. The provision of this central function by means of (qualified) electronic signatures is the crux of the Signature Directive.

Signature as a requirement for the validity of written documents (both in civil and public law) has a number of functions (such as conclusion, authenticity, warning, identity and evidence functions)[88]. In no case does the Signature Directive lead to the establishment of new rules about forms to be used in business or administrative dealings. The rules of signing documents only offer the possibility to comply with the requirements concerning documents or signatures also electronically.

No 527/2004 provides in many respects more accurate conditions with regard to electronic signatures than the Signature Act, e.g. it stipulates basic technical conditions for electronic signature.

87 Within the classified system of electronic signatures, qualified signature belongs to the highest class. For more information see section 11.2.2.

88 *Menzel*, Elektronische Signaturen (Electronic signatures), 149ff.

11.1.2 Legal communication

Electronic signature can be applied in a wide range of areas. Basically, it can be used both in private business communication and in communication with public administration. There are certain exclusions either stipulated by law or based in private arrangements.

There are several different types of communication:

- Business to Business (B2B) - Legal communication between businesses;
- Customer to Customer (C2C) - Legal communication between citizens;
- Business to Customer (B2C) - Legal communication between businesses and citizens;

Within e-Government, there are the following possibilities:

- Administration to Business (A2B) - Communication between administration and business;
- Administration to Citizen (A2C) - Communication between administration and citizens; and
- Administration to Administration (A2A) - Communication between individual authorities.

In order to achieve simplification in these areas and speed up the entire process, it is necessary to be able to conclude legally valid agreements also electronically which requires unambiguous identification. To that effect, the concept of a Citizen Card is applied in Austria which is based on electronic signature.

11.1.3 Definition

Electronic signature is defined in Article 2(1) of the Signature Directive as follows:

Electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

Therefore, the key points of electronic signature are a correct linkage between a document and its signatory and a guarantee that a signed document will not be falsified.

Thus, a signature serves to link a document with its signatory. In the case of electronic signatures, electronic data is attached to an electronic document for this purpose, on the basis of which it is possible to establish the signatory's identity and integrity of the document.

Electronic signature has nothing to do with a scanned hand-written signature (which, in fact, does not comply with complex security standards of electronic signature) or an encryption of a

legible “clear text” to make it illegible (“secret text“) (if required, electronic signature can be combined with an encryption of a legible clear text).

11.1.4 Functions

Based on the quality of electronic signature (see section 11.3), various mathematic procedures can be used to create it. They can be based on a certificate or be non-certified.

The procedure used at present to create electronic signatures uses a so-called Public-Key-Infrastructure (PKI) based on asymmetric cryptography. In contrast to symmetric cryptography, two different keys are used for encrypting and decrypting purposes: a public key for encrypting and a private key for decrypting. For the purposes of electronic signature, exactly this encrypting method is applied in the reverse order.

A certificate is used to allocate signatory’s identity in a safe manner. A certificate is an electronic attestation to which the data proving a signature (public key) of a certain person (signatory) are allocated and whose identity is documented on a certain security level (see section “Certificates” below). A certificate can also contain additional characteristics of the signatory, such as his/her profession, etc.

During the procedure, each signatory is provided a pair of keys consisting of a private and a public key. The private key may only be known to the signatory, whereas the public key to which the certificate is allocated as well is generally available and known to anybody. These key pairs have to be unique and may not exist in duplicate. Further, it must not be possible to determine the public key from the private key and vice-versa.

However, the PKI procedure is not the only acceptable procedure used to create electronic signatures. Due to the technologically neutral text of the Signature Directive, it is allowed to use other procedures as well. However, with respect to the current advanced stage and security of electronic signatures, the requirements of the Signature Directive hardly provide for any other reasonable possibility. As a result, only electronic signatures which are created by means of the PKI infrastructure should be used.

11.1.4.1 Creation of an electronic signature:

- The clear-text document to be signed by means of electronic signature is processed by hashing to produce a hashed value based on a mathematic algorithm (e.g. fhj48dhsv9bjsdk3394gaqxys9). In other words, the hashed value can also be called a “digital fingerprint” of the signed document. The purpose of the hashing function is to compress the information to a small block of interconnected data. As a result, only the hashed value and not the entire document is encrypted which has an advantage of saving resources. The hashing function is not reversible which means that it is not possible to restore the original text of the document on the basis of the hashed value.

- The hashed value is encrypted using the private key of the signatory. It is also made by means of a mathematical algorithm which is, however, only assigned and known to the signatory. As a result, the signature value (e.g. 5inbfgjuh89hucdv2) is generated.

- The signature value is added to the signature block which contains also the certificate (with a corresponding public key and the serial number) and the date.

- The signed document, which can be used further, is composed of the signature block and the (non-encrypted) document in clear text.

11.1.4.2 Verification of an electronic signature:

- From the delivered document, the addressee creates a hashed value (e.g. fhj48dhsv9bjsdk3394gaqxys9) using the same algorithm as the signatory.

- A signature value is taken from the signature block.

- The addressee decrypts the signature value using the public key of the signatory obtaining a comparative/reference value (e.g. fhj48dhsv9bjsdk3394gaqxys9).

- At this point, the hashed value generated by the addressee is compared with the comparative/reference value (decrypted signature value). If both values are identical (fhj48dhsv9bjsdk3394gaqxys9 = fhj48dhsv9bjsdk3394gaqxys9), the electronic signature is valid.

The several-step procedure and verification of signature is performed automatically using programs in the background which go unnoticed by the user.

11.1.5 Encrypting procedures

As mentioned above, the delivered document itself is not encrypted; the document is only accompanied by an encrypted hashed value (signature). The confidentiality of the document has no additional protection provided by document encrypting. However, it is always technically possible to additionally encrypt the entire document using other cryptographic procedures. For security reasons, however, it is not recommended to use the signature key created for authentication purposes to encrypt the document.

11.1.6 Information to be derived from a valid electronic signature

A valid electronic signature means that

- The signed electronic document comes from the person designated in the certificate (because it is the only person who has been provided the key pair consisting of the private and public key); and

- The signed electronic document has not been manipulated or changed (e.g. during its delivery) because any change of the document, be it a change, addition or removal of a single character, would lead to the creation of a different hashed value.

11.2 Certificates

A certificate is an electronic attestation which links identity data of a certain persons (signatory) with a public key. In addition to different information stored in certificates, there are different legal requirements related to them, such as a guaranteed security level of the creation process and the trustworthiness of the entity issuing them (certification-service-provider).

In consequence, the role of a certification-service-provider is of utmost importance for the trustworthiness of a certificate and an electronic signature created from it. Therefore, qualified certificates may only be issued by a certification-service-provider, not by anyone. These certification-service-providers are subject to state supervision (see section 11.5).

Article 6 of the Signature Directive stipulates further that by issuing a certificate as a qualified certificate to the public or by guaranteeing it to the public, a certification-service-provider is liable for damage caused to any entity or a legal or natural person who reasonably relies on that certificate.

According to Article 23 of the Austrian Signature Act, a certification-service-provider who issues a qualified certificate is *inter alia* liable for the correctness of the data provided in the qualified certificate at the time of its issue.

The combination of supervision of the issuer of certificates and liability of certification-service-providers towards a third party creates a system which makes the basic requirements for electronic signature trustworthy or, in the worst case, guarantee compensation to the user.

To fulfill their function, certificates should contain the following information:

- Name of the owner,
- An electronic signature of a certification-service-provider which protects the certificate from unnoticed changes,
- The public key of the owner.
    - The public key is added to the signature; however, there is a possibility to consult certificates in the list of certificated provided by a certification-service-provider.

11.2.1 "Simple" certificate[89]

According to Article 2 (9) of the Signature Directive, a "simple" certificate is defined as follows:

Certificate means an electronic attestation which links signature-verification data to a person and confirms the identity of that person.

Signature-verification-data mean a public key which is allocated for the purpose of identity verification of a person.

11.2.2 Qualified certificate

Unlike "simple" certificate, qualified certificate has to comply with certain requirements. According to Article 2 (10), qualified certificate has to meet the requirements laid down in Annex to the Signature Directive while certification-service-provider has to fulfill the requirements laid down in Annex II.

According to Annex I, qualified certificates have to contain:

- *An indication that the certificate is issued as a qualified certificate;*
- *The identification of the certification-service-provider and the State in which it is established;*
- *The name of the signatory or a pseudonym, which shall be identified as such;*
- *Provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;*
- *Signature-verification data which correspond to signature-creation data under the control of the signatory[90];*
- *An indication of the beginning and end of the period of validity of the certificate[91];*
- *The identity code of the certificate;*
- *The advanced electronic signature of the certification-service-provider issuing it;*
- *Limitations on the scope of use of the certificate, if applicable; and*

89 The term "simple" certificate is contained neither in the Signature Directive nor in the Austrian Signature Act; they both operate only with the term "certificate". Nevertheless, it is a common term used to better distinguish it from the second category.

90 Public Key

91 A qualified certificate has only a limited validity. It should be ensured that a certificate complies with state-of-the-art technologies and security standards.

- *Limits on the value of transactions for which the certificate can be used, if applicable.*

A qualified certificate has to be issued by a certification-service-provider who fulfills the requirements laid down in Annex II of the Signature Directive (e.g. strict technical requirements, procedures to verify the identity of the client, use of reliable staff members, as well as provisions for satisfying liability claims). To make the content of a qualified certificate trustworthy, a qualified certificate has to, in accordance with Article 5(3) of the Austrian Signature Act, be provided with a signature of a certification-service-provider which complies with the requirements of Article 2(3)(a) through (d) of the Signature Act (corresponding with the advanced signature referred to in the Signature Directive).

At present, qualified certificates are only provided by the A-Trust[92] company of all the certification-service-providers established in Austria. Other certification-service-providers offer "simple" certificates of different security levels. In this connection, it is has to be pointed out that both the Signature Directive and the Austrian Signature Act require that certificates issued by a certification-service-provider established in the EU (whose effectiveness can be verified from the EU) shall be treated as equivalent. Qualified certificates issued by such a certification-service-provider have the same legal effect as EU qualified certificates and can, therefore, be used to verify signatures in the same manner.

11.3 Types of electronic signatures

All different types of electronic signatures can be classified within one classification system of several levels. The signed documents have varying legal effects according to the security level and certificate which has been used and applied for the creation of a signature.

11.3.1 "Simple" electronic signature[93]

Article 2(1) of the Signature Directive defines "simple" electronic signature as follows:

Electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

This definition describes the basic function of an electronic signature, i.e. the verification of integrity of a signed document proving authenticity of the data. However, "simple" electronic signature does not enable to achieve secure identity which can only be achieved by complying with further requirements with regard to the signature and, in particular, to the used certificate.

In addition, the definition of electronic signature is technology-independent and is not limited to any particular signature methods. Thus, the security of electronic signatures is still based on

92 http://www.a-trust.at/

93 The term "simple" electronic signature is contained neither in the Signature Directive nor in the Signature Act; they both operate only with the term "electronic signature". Nevertheless, it is a common term used to better distinguish it from other categories.

cryptographic procedures used to create electronic signatures. In the Annex to the Austrian Signature Regulation[94], examples are provided of algorithms and parameters which are considered to be safe.

Documents which are provided with a "simple" electronic signature have to be allowed to be used as evidence which makes them subject to appraisal of evidence in legal proceedings ("non-discrimination clause" of 5(1)(b) of the Signature Directive).

11.3.2 "Advanced" electronic signature

The term "advanced" electronic signature is used to define other functions of the signature, namely its function of identifying the signatory. According to Article 2 (2) of the Signature Directive, the "advanced" electronic signature has to fulfill the following requirements:

- *It is uniquely linked to the signatory;*
  - It means that the signature may only be used by one particular person and not by any other persons at the same time. The pair of keys has to be unique for each person.
- *It is capable of identifying the signatory;*
  - Basically, the "advanced" electronic signature has to make clear the real identity of the signatory. Nevertheless, only a secure signature by means of a qualified certificate can be seen as an ideal verification of a person's identity by a certification-service-provider. Therefore, it is still not possible to speak about a secure and unambiguous identity.
- *It is created using means that the signatory can maintain under his sole control;*
  - The signatory has to have control of the access to signature creation data (private key) to be able to protect them. At present, it is achieved by saving this data on Smartcards. The signature can then be created using a certain code. It is a common view that such a control can be achieved by saving the data on a secure server. It has to be pointed out, however, that contrary to Smartcard, the signatory usually does not have any control over the use or location of the server. It is only true in cases when the server and its operation personnel are sufficiently trustworthy.
- *It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;*

94 Decree of the Federal Chancellor on Electronic Signatures (Signature Regulation – SigV), Federal Code II No 30/2000, as amended by Federal Code II No 527/2004.

- Since singed data is often exchanged through open networks, it has to be protected against manipulation. At the very least, it has to be ensured that any changes are easily detectable. To this end, technical procedures are applied. The above-mentioned PKI infrastructure seems to be appropriate in this respect.

The Austrian Signature Act does not define the term "advanced" electronic signature. This term is only to be found in the Signature Directive which defines it as an electronic signature which, compared with the Signature Act – except for Article 2(3)(e) of the Signature Act (qualified certificate and security requirements), complies with the requirement of a secure electronic signature. Thus, it is made clear that in Austria a secure electronic signature also meets the requirements of an "advance" electronic signature within the meaning of the Signature Directive.

In the European context, advanced electronic signature is to be used, in particular, for electronic billing[95]. Electronically provided invoices will be considered to be excluded from the payment or prepaid tax if they are provided with an advanced electronic signature or a qualified signature. Whereas in Germany, qualified signature is required for electronic billing, in Austria only advanced signature is necessary, according to the above-mentioned definition.[96]

In practice, there is still ambiguity with regard to identification and thus verification of invoices with regard to tax authorities, which are provided with an advanced electronic signature. In this respect, it is necessary that it is apparent to the invoice recipient whether an electronic invoice issued for him meets the criteria of an advanced electronic signature. However, it is not clear from the signature provided (and not even from the respective signature certificate) whether the requirements have been fulfilled. At present, there is legal uncertainty caused by using the "advanced electronic signature" due to insufficient requirements for the use of a qualified certificate, which could be recognizable as such by its identification, and the necessity to lay down technical procedures which would make the requirements of an advance signature verifiable and thus transparent.

11.3.3 Secure electronic signature

Based on the Signature Directive (Article 5), secure electronic signatures represent the highest level of electronic signatures. The definition is based on that of the advanced electronic signature while all the requirements of the advanced signature have to be met. In addition, the following requirements are to be fulfilled:

- It has to be based on a qualified certificate;

  Here, the requirements of Annex I of the Signature Directive with regard to the content of a secure signature apply which has significant advantages with regard

95 Directive No 2001/115/EC

96 For Austria: Regulation of the Federal Ministry of Finance stipulating the requirements for invoices submitted electronically ("Electronic Billing Regulation"), Federal Code l. II No 583/2003.

to signatory identification. The identity is verified by means of an ID only in one qualified certificate. In addition, certification-service staff members are liable for the correctness of the data.

- It has to be issued by means of a secure signature-creation device;

  A secure signature-creation device is defined in Annex IV of the Signature Directive. Secure signature-creation devices have at least to guarantee, through suitable technology and procedures, that e.g. the data used for the creation of a signature may in practice only occur once, that it is not possible to derive the key, it is possible to protect the key from unauthorized use by third parties and that it is possible to create data to be signed before the signature process. Again, these elements can only be provided by the PKI at present.

In addition to the legal effects of a "simple" electronic signature, a secure electronic signature fulfills, according to Article 5 of the Signature Directive, the requirements of a handwritten signature. These two signatures have equal legal value. In Austria, there are, however, certain exceptions which are based in particular on special requirements with regard to the form which don't concern only hand-written signature.[97]

Electronic communication thus has a suitable tool available which satisfies the requirements of an official procedure which requires that an application form be signed.

Secure electronic signatures serve both for the communication between citizens / businesses and the authorities and between citizens and businesses replacing handwritten signature. Thus, it can be applied both in the field of e-commerce and e-Government. According to Article 3(7), the Member States may *make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.*

Nevertheless is has to be pointed out that unambiguous identification is not possible only by means of a secure signature. Based on a picture ID, certification-service-providers verify the identity of a person in question and enter the data securely into the certificate, however, confusion and mistakes can not be excluded for persons with the same name or who have changed their names. For these reasons, an additional element has been introduced to secure

97 1. This applies to legal operations based on family or succession law which have to be done in writing and/or fulfil stricter requirements with regard to the form,
2. This applies to other declarations of intent or legal operations which, in order to be valid, have to fulfil certain requirements with regard to the form, such as public authentication, legal or notarial certification or a notarial deed,
3. This applies to declarations of intent, legal operations or submissions which, in order to be entered into the Land Register, Commercial Register or another public register, have to be provided with public authentication, legal or notarial certification or a notarial deed,
4. This applies to a certificate of citizenship (Article 1346(2) of the General Civil Code) which are provided by persons outside the scope of their commercial, business or professional activities.

signature in Austria, which enables an unambiguous linkage thanks to a so-called personal linkage facilitating unambiguous identification.

It is also not possible that electronic signature is created by chance. Before signing a request, it is indicated in full wording (secure indication). To create a signature, it is not enough just to have a signature-creation device, it is also necessary that a person in question knows how to create it (e.g. a code is asked).

From the data security point of view, we have to assume, based on the current state of technology, that the key length used in PKI procedures is sufficient to meet the requirements (no reciprocal derivation etc.) of secure signature. Fast-paced technological development requires, however, that the certificates be issues for five years at the most. After that, a new certificate has to be used because it might be possible that at that time longer keys will be used. However, the highest risk at present is posed by the sharing of the signature-creation device or a code necessary to produce the signature. Both are the responsibility of a signatory. Article 21 of the Signature Act stipulates the duty of a signatory to carefully store signature-creation data and, if possible, to prevent access to signature-creation data and prohibit their dissemination; however, it is in fact not possible to prevent it only by means of a legal regulation. Unauthorized sharing of codes could possibly be limited by biometric signs such as fingerprints.

11.4 Special uses of electronic signature

11.4.1 Citizen Card and personal linkage

According to Article 4(1) of the Austrian e-Government Act (E-GovG)[98], Citizen Card[99] serves during administrative procedures[100] as evidence of

- Unambiguous identity of an intervening person and
- The authenticity of electronically submitted application.

Authenticity is guaranteed by a secure electronic signature contained in the Citizen Card. Unambiguous identification of a natural person is effectuated by means of a so-called personal linkage. This step is necessary because the qualified certificate only contains the name of a person. Therefore, same names, changed names and different ways of spelling cause certain confusion when using certificates alone. Personal linkage, on the other hand, requires the use of yet another unambiguous identity sign of the person (a so-called "Stammzahl") along with the certificate.

98 Federal Act on the Provisions to Facilitate Electronic Communication with public authorities (e-Government Act – E-GovG), Federal Code l. I No 10/2004.

99 http://www.buergerkarte.at/

100 The e-Government Act allows also for the used of Citizen Card functions in the private and business spheres.

As a result, Citizen Cart is comprised of the respective certificate and the "Stammzahl" of the Citizen Card owner.

It is also not possible to imagine the implementation of e-Government without IT security mechanisms. The open concept of Citizen Card is central to the system which allows for a whole range of different technologies while guaranteeing security for all parties. A specific and openly available "Security Layer"[101] between applications and Citizen Card guarantees independency of both the system and its applications. The implementation of a standard browser guarantees security without the need of any complicated special installations and complex preconditions. It has to provide suitable identification and protection against unauthorized use.

Personal linkage provides a secure identification during electronic administrative procedures. Personal linkage and electronic signature replace insecure password systems und a single registration for each procedure. In addition, Citizen Card can also be used, under same conditions, in communication with private businesses and serve as an identification tool.

11.4.2 Administrative signature

According to Article 25(1) of the e-Government Act, Administrative signatures may be used for a certain period of time in Austria (until 31 December 2007) when using the Citizen Card function.

Until such time, administrative signatures will be legally equal to secure electronic signatures solely within the Citizen Card function. Contrary to secure electronic signature, basic organization requirements are somewhat relaxed, e.g. A1 signature[102] (as a prerequisite, the user has to have a cell phone and an Internet connection) or an e-Card[103].

Administrative signatures:

- Don't necessarily have to meet all the requirements related to the creation and saving of signature-creation data of a secure signature; and
- Not necessarily be based on a qualified certificate;
- However, they have to fulfill adequate security requirements of the Austrian Administrative Signature Regulation.[104]

The basis for the creation of administrative signature was a fee provided for at that time in the Austrian Signature Regulation[105] which was to be paid by certification-service-providers, who issued certificates, per an issued and valid qualified certificate and year.

---

101 http://www.cio.gv.at/onlineservices/basicmodules/

102 http://www.a1.net/privat/a1signatur

103 http://www.chipkarte.at/

104 Regulation on safety organizational requirements with regard to administrative signatures (VerwSigV), Federal Code II No 159/2004.

First of all, administrative signatures serve for communication from a citizen / business to the authorities where they are to be treated as secure electronic signature. If administrative signatures are used for communication between citizens and industry, this communication has no legal quality in accordance with the quality requirements laid down in the Austrian Administration Signature Regulation if they are not used, in electronic communication with a private client (industry-specific personal identifier - wbPK), in combination with identification according to the e-Government Act.

11.4.3 Official signature

According to Article 19(2) of the e-Government Act, the official signature facilitates to identify the original of a document from an authority serving as a tool for communication from an authority to a citizen (A2C) or a business (A2B). The addressee can detect that he/she received an official document. However, official signature should not be reduced to a stamp (e.g. official round stamp) of an authority; it is a signature of a natural person dealing on behalf of the authority.

Official signature has to comply with the following requirements:

- It is an electronic signature as stipulated in the Signature Act (Article 19(1) of the e-Government Act);
- Identification of origin has to be documented by means of an adequate characteristic (administrative characteristic of an authority[106]);
- It may only be used by authorities as electronic signature or for issuing document they produce (Article 19(2) of the e-Government Act);
- Official signature has to be provided (visualized) in the form of a signed electronic document (Article 19(3) of the e-Government Act);
- It has to be possible to verify the signature by means of reversing the view of the entire document (Article 19(3) of the e-Government Act).

Signaturwert	GrDUbg1TPxtqwpY4Q2AUBbZPOYIbQgCqR5zJ35jAu3uAD1Uv5vvoWqhhwg04 fWg5tg/6JE1Cqq0/EHtX4+Y5LZaCWEToVwEzQqlNdSNsy/3wYe/SRoelskSx chOYyy0VC9HT9MSvDY4h9C9PBWk3Bz5YJU10tu+58vsmVyHIKZs=	
	**Formular/Verfahren**	urn:publicid:gv.at:form+allgemeines-anbringen-test-1.0
	Datum	2003-09-27T08:33:41
	Inhaber	Dipl-Ing. Dr. Techn.Reinhard Posch
	Aussteller	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, a-sign-Premium-Sig-01
	Seriennummer	6655:859852835767

105 Decree of the Federal Chancellor on electronic signatures (Signature Regulation – SigV), Federal Code II No 30/2000, as amended by the Federal Code l. II No 527/2004.

106 For so-called object identifier (OID) of public administration see http://www.cio.gv.at/it-infrastructure/oid/

If the document is signed with an official signature and it is possible to verify the signature even in printed form by reconstructing the electronic version of the document there shall be a presumption that the paper copy of the document is genuine (Article 20 of the e-Government Act).

According to Article 19(3) of the e-Government Act, the official signature shall be represented at least by an image of the authority, the value of the signature, the serial number and the name and country of origin of the certification-service-provider.

11.4.4 Exclusive electronic signatures for authorities and professional groups

Meanwhile, the Austrian legal system provides for a number of different electronic signatures which may only be used by authorities or certain professional groups (notaries, attorneys, civil technicians) complying with certain requirements. Whereas signatures of authorities (justice and archive signatures) based on an official signature (see section 3.4.3) display a certain characteristic in the certificate (administrative competence) and, consequently, do not necessarily have to be based on a secure signature, this requirement remains valid for certain professional groups.

In order to summarize the usage of electronic signatures, we provide a general overview of the special electronic signatures and their application:

- Electronic signature of the justice

  The purpose of justice electronic signature is to be appended to electronic copies of legal documents, if it is required by the Regulation, as well as communicable versions of electronic certificates from the certification archive of the Justice Department.

- Archive signature

  The purpose of archive signature is to save an electronic certificate or to recall a communicable version of an electronic certificate from document archives of public bodies.

- Electronic certification signature of notaries

  For the purpose of electronic signing as referred to in Article 1 of the Notarial Regulation,[107] the notary is, according to Article 13(1) of the Notarial Regulation, obliged to use a secure electronic signature which is reserved to issue official documents. The capacity of a notary, as well as the contents of an official

[107] Notarial Regulation of 25 July 1871, Imperial Code 1. No 75, as amended by the Federal Code l. I No 164/2005. (Notarial Regulation)

signature shall be entered into a qualified certificate (Article 13(2) of the Notarial Regulation).

- Electronic notarial signature

  According to Article 13(1) of the Notarial Regulation, electronic notarial signature is a secure electronic signature which enables to perform official functions in accordance with Article 5 of the Notarial Regulation. The capacity (occupational title) of a notary is to be entered into a qualified certificate (Article 13(2) of the Notarial Regulation).

- Electronic attorney's signature

  Attorneys may, with the consent of a party, save for example official or private documents in an attorney's document archive after appending their electronic attorney's signature.

- Electronic certification signature of civil technicians

  For the purpose of electronic signing of official certificates issued by civil technicians, civil technicians are, according to Article 16(1) of the Civil Technician Act[108], obliged to use a secure electronic signature which is reserved to issue official documents. The capacity of a civil technician, as well as the contents of his/her signature shall be entered into a qualified certificate (Article 19(3) of the Civil Technician Act).

- Electronic civil technicians' signature

  According to Article 16(3) of the Civil Technician Act, electronic civil technicians' signature is a secure signature which may be used for the performance of the activities falling within the scope of civil technicians' activities, with the exception of signing official documents. The capacity (occupational title) of a civil technician is to be entered into a qualified certificate.

11.5 Supervision of certification services

The Signature Directive lays down in general terms the necessity to ensure supervision of certification services and thus of issued certificates. However, Article 3(3) limits supervision to those certification services which issue qualified certificates. It can be justified by the fact that only electronic signatures based on qualified certificates have the same legal effect as hand-written signatures. Certification-service-providers for "simple" of advanced signature may, but do not have to be supervised.

---

108 Civil Technician Law 1993, Federal Code l. No 156/1994, as amended by the Federal Code I No 164/2005.

In addition, according to Article 3(2) of the Signature Regulation, voluntary accreditation systems can be introduced or maintained, as appropriate, which are aimed at increasing the level of provided certification services. All requirements related to these systems have to be objective, transparent, adequate and non-discriminatory.

Article 3 stipulates that certification-service-providers only have a duty of notification. In Europe, the provision of certification services may not be subject to approval. In particular, a decision has been made to this effect that certificates which are regarded as highly trustworthy may also be issued by private bodies. To that effect, the supervisory system should function reliably.

11.5.1 Supervision authority in Austria

According to Article 6(2) of the Signature Act, a certification-service-provider shall notify to the supervisory body the beginning of its activities without undue delay. He shall provide to the supervisory body a security concept, as well as a certification concept for each of the signature or certification service offered, including any used technical components and procedures, not later than at the beginning of his activities or when any change in the activities occurs, including suspension of activities. A certification-service-provider who provides secure electronic signature procedures has to demonstrate, in his security concept, that he has complied with any additional security requirements laid down in the Signature Act.

The certification-service-provider does not have to wait for the decision of the supervisory body; he can immediately start his activities or change his activities as notified.

The supervisory body is basically involved in supervising whether the requirements of the Signature Act are complied with. Austrian system is a mixed one because it is not only certification-service-providers issuing qualified certificates who are supervised. According to Article 13(2) of the Signature Act, the supervisory body has, in particular, the following duties:

- To check the implementation of duties within the security and certification concepts;
- For the provision of secure electronic signatures, to supervise the use of suitable technical components and procedures (Article 18 of the Signature Act);
- To provide accreditation of certification-service-providers in accordance with Article 17; and
- To perform organizational supervision of confirmation bodies (Article 19).

According to Article 14(1) of the Signature Act, the supervisory body may employ measures, to ensure that certification-service-providers comply with their duties, laid down in the Signature Act or Signature Regulation. The supervisory body can, or in fact has to check the

providers based on their notification and take action with regard to supervision. In particular, it can prohibit the use, by a certification-service-provider, of inappropriate technical components and procedures or prohibit the performance of his activities in whole or in part.[109]

Further, the supervisory body can recall certificates intended for certification-service-providers or coming from signatories or instruct that certificates from signatories by recalled by a certification-service-provider.

In accordance with Article 16 of the Signature Act, certification-service-providers shall allow the staff members of the supervisory body to enter their business and operational premises during business hours for the purpose of supervision and present or provide for inspection any records or documents.

In accordance with Article 13(3) of the Signature Act, the supervisory body shall ensure that there is a register[110] of valid, blocked or recalled certificates generally available electronically for certification-service-providers at any time. In addition, the supervisory body shall ensure that a register of certification-service-providers established in Austria, certification service staff members accredited by it, and staff members of certification services of third countries, for whose certificates there is a certification-service-provider established in Austria, is generally available electronically at any time. Other certification-service-providers established abroad may be entered into the register upon request. In the certificate register for certification-service-provider, their qualified certificates will be registered so that they can provide their certification services. These certificates can also be issued by the supervisory body. The supervisory body shall provide the register maintained by it with a secure electronic signature. The certificate of the supervisory body shall be published in a bulletin of the "Wiener Zeitung" - an Austrian daily newspaper.

In accordance with Article 13(1) of the Signature Act, the supervisory body is a telecom-control-committee. For the purpose of supervision, it can make use of the Rundfunk und Telekom Regulierungs-GmbH (RTR)[111], in accordance with Article 15(1) of the Signature Act. The supervisory body is an authority which may issue official documents. The decisions

109 If no milder measures can be employed, a certification-service-provider is to be prohibited to perform his activities if:
1. He or his staff members can't prove the reliability of provided signature certification services;
2. He or his staff members do not have necessary professional skills;
3. He does not have sufficient financial resources;
4. He fails to fulfill the duties related to the performance of the activities related to the security or certification concept;
5. He fails to provide compulsory recording or recall duties at all or in a due manner or fails to fulfill the closure or recall duties (Article 9) at all or in a satisfactory manner; or
6. He fails to comply with the duty of notification in accordance with Article 6(2).
A supervisory body shall not use the possibility of prohibiting the activities of a certification-service-provider as long as milder measures can be sufficiently employed in order to ensure compliance with the provisions of the Federal Act and Regulations derived from it. In particular, it can impose obligations to be fulfilled or require that any established irregularities be remedied within a set period of time.

110 http://www.signatur.rtr.at/ShowSearchCertificatesServlet?locale=de

111 http://www.signatur.rtr.at/de/index.html

of the supervisory body are the highest decisions. It is possible to bring the case to an administrative court. In accordance with Article 20(2) of the Austrian Federal Constitutional Act (B-VG), the staff members of the supervisory body may not take any instruction with regard to the fulfillment of their function.

11.5.2 Accreditation in Austria

Certification-service-providers who issue qualified certificates for a secure electronic signature may be accredited in accordance with Article 17 of the Signature Act. The accreditation is voluntary. The requirements with regard to an accredited provider are equal to the requirements with regard to another provider of a secure electronic signature. The difference is that accreditation requires previous verification which, if successfully completed, results in a title ”accredited certification-service-provider”. Accreditation is provided by the supervisory body.

11.5.3 Confirmation bodies in Austria

Article 3(4) of the Signature Directive stipulated that the conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Members States.

The Signature Directive has identified, on the one hand, the need of verifying secure signature-creation-devices by an authority independent of signature-creators, on the other hand, provided the Member States with a possibility to decide the criteria for designation of these bodies, in particular, to decide whether they will be public or private.

In accordance with the Signature Act, the confirmation bodies have two duties:

- In accordance with Article 18(5) of the Signature Act, the confirmation bodies have to check technical components and procedures for secure electronic signatures and to confirm, by means of a certificate, the fulfillment of security requirements of the Signature Act and Signature Regulation. In this field, the confirmation bodies act completely independently. A checked device may be used for the creation of secure signatures only after its certification. The certificates issued by confirmation bodies are recognized in the entire European Economic Area by virtue of the Signature Directive.

- The confirmation bodies shall inform the supervisory body or the RTR, as appropriate. This duty is exclusively subject to private law.

In Austria, a private association Zentrum für sichere Informationstechnologie – Austria (A-SIT) was appointed as a confirmation body.[112] It is possible to have several of these confirmation bodies at the same time; however, until now there has been only one in Austria.

11.6 Data protection with respect to electronic signatures

Article 8(1) of the Signature Directive stipulates that it has to be ensured that certification-service-provider and national bodies responsible for accreditation and supervision comply with the requirements laid down in the Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It is self-evident and excludes any doubts with regard to its scope. A certification-service-provider can only use that personal data which is needed to provide the services in question.

The wording of Article 8(2) is more specific. According to this Article, certification-service-providers which issue certificates to the public may collect personal data only directly from the person in question of after the explicit consent of the person in question, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not been collected or processed for any other purposes without the explicit consent of the person in question. This requirement has also been incorporated into the Austrian Signature Act (Article 22(1)). It should for example prevent central broadly-conceived issuance of certificates to the public, without the consent of the persons in question, to be stored in Citizen Cards, social security cards, etc. It is not allowed to provide the staff members of an authority with signature certificates without their consent even it this data is openly available.

In certificates, it is possible to record a pseudonym instead of a real name while identifying it as such; therefore, a certification-service-provider has to transfer data about the identity of the signatory in accordance with Article 22(1) in case a predominantly legitimate interest with regard to such identity within the meaning of the Data Protection Act[113] is plausibly displayed. In any case there is such a possibility when concluding a contract of contacting an authority. Any such data transfer shall be documented. Only such disclosure makes it possible to use electronic signatures for identification purposes within the meaning of a signature.

In accordance with the Signature Direction, a certificate can only provide information about the name and surname of is owner, as well as an assigned public key. This public key is essential for the functioning of an electronic signature and has to be available. Otherwise, no verification of authenticity and identity is possible. Contrary to that, it is imperative that a private key corresponding with the public key be protected and, therefore, is subject to data protection. Should a private key become known, the electronic signature is not reliable any more and can be easily abused. The management of personal linkage developed in connection

112 Decree of the Federal Chancellor on establishing whether the association "Zentrum für sichere Informationstechnologie – Austria (A-SIT)" is qualified to act as a confirmation body, Federal Code. II No 31/2000.

113 Federal Act on Personal Data Protection (Data Protection Act 2000 - DSG 2000), Federal Code. I No 165/1999, as amended by the Federal Code l. I No 13/2005.

with the Citizen Card concept, in conformity with data protection requirements, and further processing of this data is described below.

Any other data which the owner of a certificate wishes to indicate in his certificate (e.g. a limit not to be exceeded in a transaction) may be recorded upon request, while it is assumed that the owner agrees that the data can been openly seen.

However, any other national requirements of notification or cooperation of a certification-service-provider with respect to courts or other authorities have to remain unaffected.[114]

12 Identity management and personal identifiers

12.1 General provisions

IT security and data protection play an important role in e-Government. Citizens who want to make use of e-Government applications believe that electronic official channels are secure and reliable just as regular channels are. It is expected that public administration ensures a high degree of data protection and a responsible management of data. The high credit that public authorities enjoy has to be warranted also in e-Government by means of adequate measures.

Secure on-line procedures and network and information security are ensured by means of different measures and tools. Specially developed on-line applications, Citizen Card with personal linkage, administrative signature, sector-specific personal identifiers, use of official certificates and electronically signed documents are only some of the instruments which should contribute to continuous increase in citizens' trust in official electronic procedures.

Security has increasingly been part of current fundamental challenges. The massive proliferation of e-Government has made it a critical infrastructure which is worth protecting. In doing so, it is necessary to take into account its central components such as different registers. Any unauthorized access, no matter how insignificant, may lead to uncertainty felt by citizens and ultimately compromise the trust attached to electronic public services. A sufficiently safe and protected system may counteract these fears and lead to a broad acceptance of the entire system of e-Government.

The application of internationally recognized XML standards promotes process decoupling and decentralized automation. Therefore, XML standards and electronic signatures or resulting mechanisms of trustworthiness and data protection, to be exact, enable the implementation of e-Government which is not centrally vulnerable. The authorities would like to see that e-Government is widely accepted among citizen because only its wide use can make it increasingly cost-effective.

Since decades, data protection has played an important role in Austria. This tradition should also be pursued in e-Government. Cooperation with the Data Protection Authority has led to a

114 Cf. Article 22(3) of the Signature Act.

data protection situation which is acceptable for everybody and which uses a so-called “ZMR-Zahl” as a basis for on-line procedures.

12.2 Austrian model

12.2.1 The “Stammzahl” (*Stem code*)

Electronic affairs that the authorities deal with have to be unambiguously attributable to citizens. This unambiguous identification of persons is possible by means of a so-called “Stammzahl”. The “Stammzahl” is saved on Citizen Card which is the only place where it can be saved permanently. Thus, it is under the exclusive control of citizens.

The “Stammzahl” is calculated on the basis of a so-called “ZMR-number” which is a unique number allocated to each individual resident in Austria. For individuals without residence in Austria, the number from the Supplement Register serves as a unique identification characteristic. The “Stammzahl” and the sector-specific personal identifier (bPK) are constructed as follows:

- The “ZMR-number” consisting of a 12-digit decimal number which is converted into a binary code.
- The calculation base is increased by means of a seed-value known only to the “Stammzahl” Register Office.
- The increased binary code is then encrypted by means of a secret key which is only known to the Stammzahl Register Office.
- The Base64-Standard software is used to encrypt the result.

As a result, a 24-digit alpha-numerical character string is generated which is recorded on the Citizen Card:

Basiszahl	000247681888 (Bsp: ZMR-Zahl, 12-stellige Dezimalzahl)
Binärdarstellung	00 0E C3 53 60 (Binär 5 Byte [Darstellung: hexadezimal])
Verbreitern auf 128 Bit	00 0E C3 53 60 FF 00 0E C3 53 60 00 0E C3 53 60 (Binär 16 Byte, Seed-Wert beispielhaft auf 'FF' gesetzt)
Triple-DES Verschlüsselung	42 AD 37 74 FA E0 70 7B 31 DC 6D 25 29 21 FA 49 (Binär 16 Byte)
Base64 Kodierung	MDEyMzQ1Njc4OWFiY2RlZg== (Alphanumerisch, 24 Zeichen)

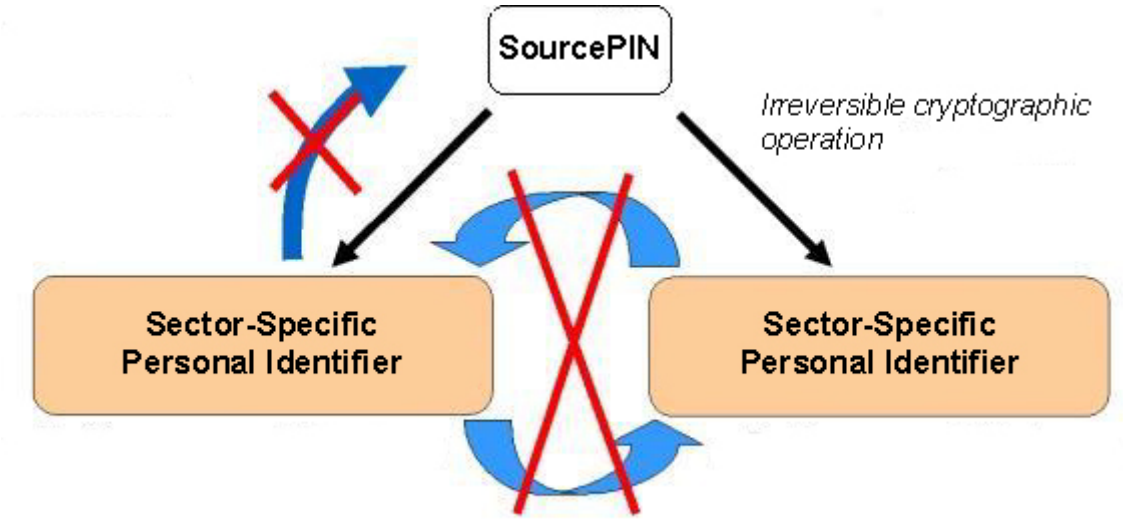
Sourse: Hollosi/Hörbe, SZ-bPK-Algo V1.0 2.2.2004. The provided values serves as an example and have not been achieved as a result of calculation.

For non-natural persons, e.g. companies, associations, etc., the serial number from the respective basic register, e.g. Commercial Register, Associations Register, etc., is used to calculate the “Stammzahl”. Thus, the “Stammzahl” of a company is its number in the

Commercial Register and the "Stammzahl" of an association is its number in the Associations Register. This number is used openly, rather than being encrypted according to different sectors.

12.2.2 Sector-specific personal identifier (bPK)

In order to ensure data protection, the use of a uniform personal identifier has been abandoned in the procedure provided within the framework of Austrian e-Government. Instead, the authorities generate different personal identifiers which are individually derived from the "Stammzahl" of the **natural person** in question for each individual sector. It is based on cryptographic one-way derivation which is irreversible. It means that it is not possible to reconstruct the "Stammzahl" based on such derivation. Nor is it possible to calculate the derivation for another sector by means of an already available derivation.



it´s impossible to derive a new identifier for another sector from an existing derivation

For data protection reasons, the "Stammzahl" of **natural persons** may in no case be saved by authorities as an identification characteristic. Should Citizen Card be used for signing an electronic request, the "Stammzahl" will be readout from the Citizen Card in step II which will be automatically followed by deriving a sector-specific personal identifier (bPK).

The resulting sector-specific personal identifier will be calculated cryptographically from the "Stammzahl" for a specific sector[115] the authority is involved in. Thus, after the procedure has been terminated, the authority will only have the sector-specific personal identifier of the person relevant for the sector in question.

When deriving a sector-specific personal identifier, a character string is generated based on the "Stammzahl" and the sector in step I. This character string is used to calculate a secure cryptographic one-way derivation using a certain hashing algorithm. For the purpose of

[115] See Section 2.8.3.

creating a paper copy of the document, the sector-specific personal identifier is coded using Base64- Standard software:

Stammzahl	MDEyMzQ1Njc4OWFiY2RlZg== (Base64, 24 Zeichen)
Bereichskürzel	BW (ISO-8859-1, Beispiel: Bauen und Wohnen)
Zeichenkette	MDEyMzQ1Njc4OWFiY2RlZg==+urn:publicid:gv.at:cdid+BW
SHA-1	312c103b f5213b94 46fa747e 92568e4e c558f825 (5x32bit [Darstellung; hexadezimal])
Base64	MswQO/UhO5RG+nR+klaOTsVY+CU= (28 Zeichen, ISO-8859-1)

Sourse: Hollosi/Hörbe, SZ-bPK-Algo V1.0 2.2.2004. The above-provided values serves as an example and have not been achieved as a result of calculation.

Contrary to natural persons, the sector-specific personal identifiers of persons who preside over different bodies have to be reversible, in accordance with e-Government Act, which should ensure that state actions can be traced back. In this case, the sector-specific personal identifiers can only be created upon inquiring the "Stammzahl" Register. To calculate these sector-specific personal identifiers, a symmetric encryption with a secret key known solely to the "Stammzahl" Register Office is used instead of one-way derivation. The result is coded.

For non-natural persons, there is no derivation because in their case their "Stammzahl" is used as a uniform identifier.

- **Industry-specific personal identifiers**

The method of sector-specific personal identifiers used for identification of persons can also be used in trade and industry for electronic business. Contrary to public administration, industry-specific personal identifiers (wbPK) are based on the "Stammzahl" of the client which indicate the sector. In order to create an industry-specific personal identifier it is, therefore, necessary to use both *stem codes* which should ensure that the person in question knows and agrees with the creation of an industry-specific personal identifier. In this case, it is not possible to read the "Stammzahl" for the creation of an industry-specific personal identifier electronically; rather, it is taken from the environment of the Citizen Card and used to create a sector-specific personal identifier. Thus, each business or association makes up its own sector.

- **Information provided to another sector**

Should an authority need a sector-specific personal identifier from a different sector (Fremd-bPK) to identify a person, it may be inquired from the "Stammzahl" Register Office. The Stammzahl" Register Office provides the required information about the sector-specific personal identifier (Fremd-bPK) exclusively in an encrypted manner. Therefore, the "Fremd-bPK" may only be decrypted by the authority which is responsible for the other sector for which the "Fremd-bPK" was created. The calculation of an encrypted sector-specific personal

identifier has to be performed in such a manner so as to exclude the possibility of identifying the person in question.

12.3 The Czech model

In the Czech Republic, there are e-Government applications based on electronic signatures available. Because, during implementation of these applications, it is inevitably necessary to unambiguously identify a person contacting an authority, the Czech Identity management, in its current form, has to be provided certain information about the Austrian view with regard to this topic.

At present, a uniform personal identifier[116] is used in the Czech Republic. The number, known also as a "birth ID number" is comprised of a 10-digit string of numbers which consists of the following elements: year of birth (2 digits), month of birth, day of birth and a 4-digit number without reference to the personal data of the person, which serves both for identification and checking purposes. According to the effective legal rules and regulations, this number may be processed in legally indicated cases or if a person has agreed to such a processing of his/her "birth ID number". The "birth ID number" is mostly used for public administration purposes; however, it may also be used privately.

Basically, with respect to its functioning, a combination of the "birth ID number" and a secure electronic signature fulfills the basic requirements of an identity management system, i.e. to be able to identify a person unambiguously and ensure authenticity of transfer. However, data security concerns see certain problematic areas in the system.

Since computers have increasingly penetrated all aspects of our lives, it seems that a uniform unambiguous personal identifier is not an ideal option with regard to data protection because whoever knows the unambiguous identifier of a person may find that person on the basis of the data using the identifier without any trouble. The risk of abuse related to the exchange of data with other clients, without consent of the person in question, is increased due to the fact that it is easier to compare the data on the basis of an unambiguous identifier. It is also true that the more an unambiguous identifier is spread the higher is the natural interest to both use and abuse it.

The data protection issue we are facing here is that it is extremely difficult to prove an abuse but most importantly it can't be effectively prevented. This problem is present with any form of unauthorized data transfer, however, it is much more serious when combined with an unambiguous personal identifier which may be used in all public and private areas where electronic data is used.

Therefore, the Austrian legislators decided to develop the above-mentioned model of sector-specific personal identifiers (bPK) and to authorize a data protection committee to take over

116 Zákon č.133/2000 Sb. (Act No 133/2000 Coll.)

the supervision and control of data transfer using these sector-specific personal identifiers. The method is based on the following steps: the "Stammzahl" Register Office of the Data Protection Committee first checks the use of data by a particular client (public authority) which seeks to equip these particular data uses with sector-specific personal identifiers before sector-specific personal identifiers can be allocated to the data uses. After the data uses have been equipped with sector-specific personal identifiers, abuse can be traced any time by means of the evaluation of protocols created during the calculation of a sector-specific personal identifier or a "FremdbPKs" because the "Stammzahl" Register Office has the key necessary for the functioning of the system available. Data transactions which are considered to be unauthorized by the Data Protection Committee can be eliminated by failing to provide a "Fremd-bPK" to the client.

Austria has decided not to allow any unambiguous personal identifiers to be used outside the public sector, which could be used or provided by means of re-calculation to any different areas. Private institutions may in fact identify their customers by means of Citizen Card and thus achieve an unambiguous identification of their customers, however, they can't use these identifiers, designated solely for the use in their sector, in any other area because they are not able to derive a "Fremd-BPKs" from these sector-specific personal identifiers.

At first glance, it seems appealing to use open personal identifiers established for e-Government also for private purposes, however, if we do not take account of the data protection concerns mentioned above, there are still some legal boundaries outlined in the following paragraphs.

In accordance with Article 7 of the Directive 95/46/EC, consent is needed for storing and processing of personal identifiers while no particular rules are laid down for the storage time period processing method. When deciding what was the wish of the person in question it has to be considered that a uniform identifier make comparisons of data much easier; however, the usual procedure will be that communication of a „birth-ID-number", should data transfer be possible, is not allowed because the only advantage of communicating this number is in easier comparison of data. It is a legitimate interest of each person in question that his/her profiles are created as rarely as possible. Explicit consent is only given in those cases when the person has been provided detailed information about comparison of data with other data for the purpose of profile creation. As a rule, it is not possible to provide such consent in the public sphere due to the relation of dependency but quite often it is not allowed in the private sphere due to the relation of subordination or superiority either[117].

Surely, it is difficult to ensure control and/or detect unauthorized data processing, in particular data transfer, in an open system. However, it is for this reason that stricter checks are necessary mainly, but not only, for the reason of general prevention since regular abuse would jeopardize the right of citizens to personal data protection because the cases of non compliance with data protection requirements are difficult to reverse.

117 For futher evidence, see the information of the Austrian Data Protection Committee K178.209/0006-DSK/2006.

Finally, the observance of basic data protection principles during the implementation of identity management is a prerequisite for the proper functioning of the system and, consequently, a cornerstone of its future success based on the regular use of the new offer.