Legal Aspects and Privacy Protection in RISER

1. Why does ICPP participate?

Quite often we are asked why ICPP participates in a project such as RISER. First of all, the legislator has provided for resident register inquiries in most of the European countries. And thus being lawful there are already companies engaged in this field, even though they are doing business mostly on a national scale. But apart from the question whether or not inquiries should be allowed – ICPP strongly believes in promoting good and most of all preventive privacy protection solutions. This is an opportunity we clearly detect in the RISER project.

2. Main Objective

The main objective of the Registry Information Service on European Residents is to give European citizens and companies the opportunity to electronically achieve official register information on a trans-European scale. In order to do so, not only secure technical solutions had to be found. Besides the technical challenge to build a secure and easy to use internet service and to implement high privacy protection standards, the legal requirements of the countries connected to the service had and have to be observed. Every single European state has its own register law let alone Germany with its federal states having quite similar but still divergent state regulations. This is an enormous challenge.

Internet Service

Being an internet service and thus using a web portal the service has to meet specific legal requirements on different legal levels. Whereas the design of the service leads to certain legal requirements governed by data protection law, other areas are affected by the service procedure itself.

The service provides pan-European address information. Therefore legal competences of different countries need to be taken into account. Since the service is established in Germany, German law is applicable to the service procedure, as RISER offers an electronic information service under the Teleservices Act.[1]

Personal data on the customer and personal data on the person being subject of the inquiry - name, address and date of birth – are data of content to which data protection law is applicable. Personal data on the customers are subject to German law because they are processed by the service provider being established in Germany. Today, as we are focusing on civil registration, I will concentrate only on aspects concerning the processing of personal data of the searched for person. Though, I would like to stress again that this is only one part of privacy protection in an e-service such as RISER.

3. Processing Personal Data

Processing personal data to forward address information affects two major fields of law: data protection and civil registration law. From a European perspective we find most

[1] Section 4 (1) Teleservices Act.

heterogeneous conditions in civil registration while the implementation of the European Data Protection Directive[2] into national law has harmonized the national data protection laws.

3.1 Legal requirements in civil registration law

In a short overview one can state certain categories of legal requirements in European register laws. Concerning the data subject it is a common requirement that it has to be identified unambiguously by the register. Concerning the inquirer most states apply different rules according to whether a company or a private person is inquiring. I will focus only on companies, as they are subject to data protection regulations. Some states, e.g. Austria, require a formal registration of the company inquiring and moreover most of those require a specific legal or acknowledged interest. Others, e.g. Germany,[3] do not require a formal registration at all but identification for reasons of encashment.

It would have been easy to add up all those single requirements and build one single web-form leaving it to the customer to gather all information whether or not necessary for his or her specific inquiry. Yet, it is one objective of the RISER project to build an easy to use interface for its customers and another to accomplish high data protection standards. Providing information that is not necessary for a specific inquiry puts an additional burden on the customer who is trying to make his or her life easier using the service. On top of that, to process as few data as possible is one of the top principles in privacy protection. To meet these demands the service is forced to use specific web-forms depending on the country the inquiry is aimed at. This also ensures that only the necessary and only as few data as possible are passed on as well as it gives relief to the customer.

3.2 Privacy Protection

Even though register law is heterogeneous there is a common instrument that allows a rather homogeneous solution. Since the European Data Protection Directive provided for data processing on behalf of the data controller,[4] this instrument is available in all European countries. The design is relatively simple and efficient. The registered RISER customer who already is in possession of some data on the data subject stays in control and is responsible for the data processing, that is, the transfer to the service and its forwarding to the respective national register. RISER on the other hand is bound by contract to the instructions of the controller which are in this case restricted to forwarding the inquiry to the competent authority and receiving the information. Thus RISER is acting somewhat like a postal service. This ensures that the inquiry service is neither allowed to store the data permanently and therewith not to build a central European Register, nor to use it other than instructed.

The basic requirement to process personal data lawfully on behalf of the RISER customer depends on the actual design of the service. It has to be based on a written contract binding the processor to the controller and stipulating the particulars. The contractual relationship between the customer and the service provider needs to conform to the requirements that are necessary to classify the service as a commissioned work according to the law of the country the customer is established in. It is decisive that the processor is only allowed to act on instructions from the customer. In RISER contracts it is therefore stipulated that RISER is only allowed to forward the inquiry to the competent authority and receive its answer.

---

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

[3] Even though some German states, e.g. Schleswig-Holstein and Hamburg, have implemented a registration for online enquiries, it is not a prerequisite according to the framework legislation which has not been implemented into all state laws.

[4] Art. 17 of the European Data Protection Directive 95/46/EC.

As personal data are processed on behalf of the RISER customer, he or she stays responsible for compliance with data protection laws and is therefore called "controller". The controller is legally liable confronting the data subject. It is the obligation of the controller to select the processor carefully.

The contractual content stipulates the kind and scope of processing personal data, the technical and organizational measures, as well as any sub-commissions. The kind and scope of processing personal data comprehends the forwarding of the address inquiry to the locally competent authority in the required form, receiving the answer and to hold it ready for customer download. In this context it is interesting to note that it is necessary to determine special contents according to the national law of the countries receiving inquiries. This affects for example whether or not a chain of addresses shall be permitted. To go on inquiring after a data subject after receiving the information he or she moved to a different city, is a separate decision and going beyond the basic commission and therefore may need a special order as e.g., in Germany.

In Germany the scope of work that may be transferred to a processor is limited. A processor turns to being the data controller itself if tasks are assigned that go beyond its function to help with data processing. This is the case whenever business functions are transferred.[5] This implies for RISER that the service is only allowed to forward the inquiry to the register authority of the last known place of residence or if, and only if, chains of addresses are allowed by the controller, to follow the trace: "Find data subject A in city[6] X and trace". RISER may not forward address inquiries on its own decision. Therefore the commissioned order cannot be "Find data subject A, no matter how". This order would definitely go beyond the scope of a commissioned work.

The processor also has to implement appropriate technical and organizational measures to protect personal data.[7] These depend on the legal requirements of the country the service is established in which, in this case, is Germany. The technical and organizational measures have to cover the complete period of time the commissioned work is running, that is from upload of data to the download by the customer. The method of transfer, storage, up- and download, erasure of personal data, and the authorized personnel, as well as maintenance[8] have to be stipulated.[9] The technical and organizational measures taken by the processor have to be laid down in a security concept that needs to be incorporated in the contract.[10]

It is prohibited for the processor to give the personal data to any third party other than stipulated. Also the persons employed in data processing are not allowed to collect, process, or use personal data without authorization based on the principle of confidentiality. Not only actions that are not authorized by law are prohibited, but also those contravening the orders of the controller. It is further necessary for the processor to give an undertaking to maintain such confidentiality to the employees taking up their duties. This undertaking needs to be valid until after termination of their activity with the processor.[11]

---

[5] Simitis a.o., BDSG/Walz, Sect. 11 no. 18.
[6] In countries that do have central registers the city may not be an obligatory datum, such as is he case in Austria.
[7] Cf. Art. 17 (3), (1) 95/46/EC.
[8] Simitis a.o., BDSG/ Walz, Section 11 no. 87.
[9] Simitis a.o., BDSG/Walz, Section 11 no. 50.
[10] Sect. 11 (2), 9 1st sentence BDSG.
[11] For Germany Section § 11 (4) in connection with § 5 BDSG.

It is the responsibility of the processor to take the appropriate measures to provide for data security.[12] If the effort involved is reasonable in relation to the desired level of protection, the personal data shall be protected against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other forms of processing.[13] The processor is under this obligation even though the controller fails to give the appropriate instructions. Further, it is the responsibility of the processor to ensure that the data is processed according to the orders given by the controller.[14]

As the processor, PSI, is established in Berlin, Germany, the German Federal Data Protection Act is applicable. The BDSG provides for a number of detailed requirements implementing Art. 17 (1) of the European Data Protection Directive[15] in an annex to the relevant Section 9 BDSG.[16]

Further more the contract stipulates the right to control the processing of inquiries as well as the right of the processor to give information on its inquiring customer to countries that provide informational rights to the data subject.

The PSI being the processor and being established in Berlin, Germany, is supervised by the Data Protection Commissioner of Berlin.[17]
Subject to monitoring is the implementation of data protection law.[18] The PSI and the persons responsible for their management have to provide the supervisory authority on request and without delay the information necessary for the performance of their duties.[19]

In particular the supervisory authority may instruct that measures are to be taken in order to rectify technical and organizational irregularities that have been discovered checking the measures set out in Section 9 BDSG.[20]

4. Advantages

An advantage of such a design is that the service is not allowed to build up a European Central Register. The service is not allowed to store the data permanently. It is only allowed to store the data as long as necessary for winding up the order. Even though the registers are easier to address because of this pan-European service, they have to be address separately. To search for somebody without having a clue to his or her residents therefore is still quite costly.

Processing data on behalf of the data controller most effectively protects the rights of the data subject towards the service. On the one hand the data controller stays responsible for the whole processing. And moreover, the RISER customer is, as he or she has to contractually confirm, legally allowed to process the personal data at stake. On the other hand the service is not allowed to either buy or sell addresses. Personal data therefore is not disclosed to third parties.

---

[12] Art. 17 (1), (3) of Directive 95/46/EC; for Germany Section 11 (4) in connection with Section 9 BDSG.
[13] Art. 17 (1), (3) of Directive 95/46/EC.
[14] Simitis a.o., BDSG/Walz, Section 11 no. 67.
[15] Directive 95/46/EC.
[16] For details, see 2.3.
[17] Sect. 33 (1) Data Protection Act of Berlin.
[18] Sect. 38 (1) BDSG.
[19] Sect. 38 (3) BDSG.
[20] Sect. 38 (5) 1st sentence BDSG.

Over and above the afore mentioned, some registers, e.g. the Austrian ZMR[21], only give information to companies that are entitled to receive the information due to legal or other interests. In these cases a service selling and buying addresses would not be entitled to register information. In these cases a mere technical provider acting on behalf of an inquirer is generally a lawful alternative.

5. Territorial Competence Concerning the Parties Involved

Registers often mention the question by whom and how to execute control. The RISER service itself is under control of the national authority which is the privacy commissioner of Berlin as the service is established in Berlin. He supervises technical security and organizational measures according to the national law. The RISER customer is supervised by his or her competent authority.[22]

Whether or not the supervision is actually executed naturally depends on the practices in the respective country. If for example the Austrian Central Register has reason to believe a German RISER customer is misusing Austrian data, it will not be able to control or enforce measures on German territory. Yet, the German authority[23] may be requested to exercise its powers by the Austrian authority (Amtshilfe). According to the European Data Protection Directive (Art. 28 (6) of Directive 95/46/EC) the supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties. Since mutual assistance is provided for in all national data protection laws due to the implementation of the directive, to exercise control on a European scale is possible even though it is has not been on the daily agenda of national data protection boards.

6. Accomplishments & Perspectives

As Europe is growing and market situations afford more or even frequent changes in ones place of residents even beyond national boarders, there is a growing demand for address inquiries.

The RISER service is one of the first e-Government solutions on pan-European scale. Offering a service that hides national diversities from the front end user, RISER takes a huge step towards a Europe that respects and incorporates national legislation.

Civil rights are always at stake where centralization takes place. To protect the rights of citizens without putting impediments on businesses will be the golden bridge. The design of RISER shows, that privacy rights and business demands may well work together. To standardize good privacy protection solutions and foster their proliferation is one aim ICPP believes in. As a Privacy Commissioner I would wish for more business solutions that would make privacy issues a part of their innovation concept.

---

[21] Section 16a (5) Austrian Civil Register Act (Meldegesetz 1991, BGBl. Nr. 9/1992, BGBl. I Nr. 10/2004) 1991.

[22] Cases such as the Danish, in which every collection of data in Denmark is subject to Danish law (§ 4 (3) No. 2) even though further processing takes place on the territory of another country, can only be solved by interpreting the law according to the prerequisites of the Directive.

[23] § 38 (1) s. 4 BDSG.