Directive

for the transfer of personal data

to third countries outside the EEA

(Munich Re reinsurance group directive on third-country data transfer)

Information correct at 1 July 2013

Contents

1 Introduction

Modern information and communications technology is giving rise to both technological and economic change. The extent and the consequences of these changes are gradually becoming apparent and can be compared to the transformation from agricultural to industrial society. Access to the Internet, access to information via the WorldWideWeb (WWW), use of electronic mail and messages, global dialogue and exchange of information: all these operations are now essential for exercising virtually any economic activity and indispensable if a company is to establish itself in the market, wishes to react rapidly and flexibly to new influences, and desires to offer an extended service both internally and externally.

It is precisely the merits of electronic communication which also make it vulnerable. The almost unlimited possibilities of processing data expose it at the same time to the risk of unauthorized alteration; its transportation via public networks allows its undiscovered disclosure to almost anybody; a computer system with access to international networks is open to access from such networks for manipulative purposes as well. The opportunities offered by the worldwide exchange of data should not be jeopardized by any infringement of rights of personality and copyrights or by disclosure of company secrets.

The planning and introduction of new information technology systems (IT) should therefore be accompanied by the checking and possibly the adaptation of existing security measures. This requirement follows, for one thing, from the company's interest in avoiding any serious damage as far as possible. For another thing, legal regulations have to be complied with as well, especially those protecting the consumer, such as the EU Directive on Data Protection and its requirements at European level and the German Federal Data Protection Act ("Bundesdatenschutzgesetz" – BDSG) or equivalent laws at national level. Under this legislation, technical and organizational measures also have to be taken to protect the data of clients, prospective clients and staff members, so that any infringement of rights of personality is avoided. But if rights of personality are to be protected, this also involves taking into account the interests of clients with respect to data protection. For any company operating on a worldwide scale such as the Munich Re reinsurance group, such protection is an essential element of its corporate policy. To ensure, irrespective of existing legal regulations, an equal level of data protection worldwide within the group, Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München or its RI group company units undertake(s) to comply with the following criteria.

2 Objective of the directive

The objective of the directive is to establish equal data protection and data security standards, in accordance with the EU Directive on Data Protection, for the processing of data within the RI group in respect of the transfer of data by company units in EEA states (see Annex 3 of the directive) to third countries thus ensuring an adequate data protection level for these bodies or providing sufficient guarantees with regard to the protection of the rights of personality and the exercise of the rights involved.

3 Scope of the directive

The directive is a framework directive and is applicable to the transfer, including the subsequent processing, of personal data of staff members, clients (members of company health insurance funds, borrowers, deposit account holders, debtors, tenants, policyholders), intermediaries and other data subjects, especially in connection with the implementation of the contract and claims settlement (claimants, shareholders, building society savers, contributors, beneficiaries, victims, suppliers and their clients, potential clients, experts, persons insured, witnesses), by RI group company units, irrespective of the legal basis for the transfer of data[1].

The regulations contained in this directive are binding for all RI group company units. Companies not belonging to the RI group may also undertake to comply with the regulations on a voluntary and legally binding basis; otherwise, this directive is not applicable to them. In this case the admissibility of the transfer of data shall be ascertained in each individual case and, if necessary, ensured by appropriate measures. In the case of revocation of the formal obligation, the obligations arising from this directive shall remain valid for any processing of personal data transferred which took place until the date of revocation.

The directive shall be applicable to the transfer, including the subsequent processing and use, of personal data by RI group company units within the EEA to those in third countries.

Existing legal obligations shall not be affected by this directive. If such obligations in third countries are in contradiction with the duties arising from this directive, the RI group company unit in the EEA carrying out the transfer shall be informed of this, even if such obligations arise subsequently.

4 Definitions

For the purposes of this directive:

- **Personal data** shall mean any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, e.g. by reference to an identification number.

- **Transfer of personal data** shall mean the disclosure of personal data, its dissemination or any other form of making it available to third parties.

- **Processing of personal data** shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission or blocking, erasure or destruction.

[1] In addition to compliance with the regulations of this Directive, a legal basis is also necessary for data transmission.

- **Controller** (controlling body) shall mean, with respect to third persons, the legally independent company of the Munich Re reinsurance group (hereafter RI group) whose business activity has caused the disclosure of data. Dependent branches form a part of the controlling body.

- **Processor** shall mean a natural or legal person which processes personal data on behalf of a controlling body.

- **Third party** shall mean any natural or legal person who/which does not belong to the controlling body.

- **Consent** shall mean a freely given and informed indication of the data subject's wishes by which he/she signifies his/her agreement to personal data relating to him/her being processed.[2]

- **Clients** shall mean natural persons with whom a business relationship exists or is intended.

- **Intermediaries** shall mean natural persons whose activity consists in negotiating insurance products and/or financial services products.

- **Third country** shall mean any country outside the European Union/the EEA.

- **Delegation of functions** exists if, in particular, distribution, portfolio management, loan assessment, claims handling, accounting, investment or asset management of an RI group company unit is permanently transferred either completely or to a significant extent to another RI group company unit.

5 Admissibility of data processing

The processing of the data mentioned in item 3 shall only be allowed if the general criteria of admissibility, i.e.

- consent,
- permissibility or
- other legal provisions

are met. This shall be a prerequisite for any export of data. Basically, general regulations shall be applicable to the processing of data on behalf of a controlling body and to the delegation of functions as well. Such regulations derive from the law of the EEA state in which the controlling body has its head office.

[2] Special requirements for any consent may arise from the national law concerned.

6 Principles applicable to the transfer and subsequent processing and use of personal data

6.1 Purpose

Personal data may only be collected and processed for specified, explicit and legitimate purposes. RI group company units or companies in third countries that have voluntarily undertaken to comply with the regulations of this directive shall be obliged to observe this purpose of the transferred data with respect to its recording and further use. Any alteration of the purpose shall only be allowed with the consent of the data subject or if permitted by the respective national law of the exporter.

6.2 Data quality

Personal data must be accurate and – where necessary – kept up to date. Reasonable steps shall be taken to ensure that data which is inaccurate or incomplete is rectified or erased. The data must be needed for the purpose in question.

6.3 Transparency

Natural persons whose personal data are disclosed by an RI group company unit in an EEA country to an RI group company unit in a third state shall be provided with the following information:

- identity of the controlling body in the third country;
- purpose of the transfer;
- other information if this is required for reasons of equity, e.g.
  - rights of access, rectification and erasure
  - right of objection in the case of advertising.

No information need be provided if

- this is necessary for the protection
  - of the data subject or
  - of the rights and obligations of other persons;
- the data subject has already been informed;
- this would involve disproportionate expenditure;
- the data are accessible to the public and information would be disproportionate due to the multitude of cases concerned.

6.4 Security

The controlling bodies shall take appropriate technical and organizational measures to ensure the required data security. Measures refer in particular to computers (servers and workstations), networks or communication links as well as applications. A catalogue of measures is enclosed in **Annex 1**.

6.5 Confidentiality of processing

Only authorized persons and staff members especially committed to complying with the provisions of data secrecy shall be allowed to collect, process or use personal data. This prohibits any use of such data for private purposes, its transmission to unauthorized persons or its being made available to such persons in any other way. For this purpose, staff members, for instance, shall also be unauthorized persons unless their scope of responsibilities and actual tasks require otherwise. A specimen of such a formal obligation is enclosed in **Annex 2**.

The obligation with regard to confidentiality shall continue even after the employment relationship has been terminated.

6.6 Data processing on behalf of other bodies

If RI group company units or companies that have voluntarily undertaken to comply with the regulations of this directive act as principals and agents under an agency contract with respect to the processing of personal data, the following provisions shall apply:

- It shall be ensured that the agent chosen takes any technical or organizational security measures required for processing.
- The carrying-out of data processing on behalf of another body shall be dealt with in a contract which is either in writing or documented in another way and which stipulates the rights and obligations of the agent.
- The agent shall contractually undertake to process any data received from the principal only within the scope of the agency contract and of the instructions given by the principal. Any processing for own purposes or for purposes of third parties shall be contractually excluded.
- The principal shall continue to be the contact for the client, staff member, etc.

7 Rights of the data subject

With regard to the personal data relating to him/her, the client, staff member, intermediary or other data subject (cf. item 3) shall be granted certain peremptory rights:

- He/she may demand **information** (possibly even in written form[3]) on the data recorded on his/her person, on its source and on the purpose for which it has been recorded.

- In the case of data transfer, he/she may require **information** on the recipients or categories of recipients as well.

- He/she may not demand information if this involves the disclosure of business secrets.

- He/she may demand **rectification** if it is shown that the personal data relating to him/her is inaccurate or incomplete.

[3] The information shall always be given in writing.

- He/she may demand the **blocking** of his/her data if neither its accuracy nor its inaccuracy can be established.

- He/she may demand **erasure** of his/her data if the processing of the data was inadmissible or if the data are no longer required for the purpose of processing. If there are legal storage requirements, the data shall be blocked instead of erased.

- He/she shall be granted a right of objection if his/her data are used
  - for purposes of advertising or
  - for purposes of market and public opinion research.
- Moreover, he/she shall be granted a general right of objection which has to be taken into account if an evaluation shows that any interest of the data subject worthy of protection prevails over the interest of the controlling body, owing to the specific individual situation of the data subject.

He/she may exercise his/her rights resulting from this directive also with respect to the transferring body.

8 Disclosure of data

8.1 Transfer of data from the EEA to other countries

The transfer of personal data from an EEA country to a country outside the EEA shall only be allowed, with due regard to item 5,

- if the data subject has given his/her consent unambiguously to the proposed transfer; or
- if the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken at the instigation of the data subject; or
- if the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded in the interest of the data subject between the controller and a third party; or
- if the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims in court; or
- if the transfer is necessary in order to protect the vital interests of the data subject; or
- if the recipient country/the receiving body ensures an adequate level of data protection for the purposes of this directive[4]. If the recipient of data is a company which has to comply with this directive, it is not necessary to check whether there is an adequate level of data protection[5]; or
- if the controlling body provides sufficient guarantees with regard to the protection of the right of personality and the exercise of the rights involved. If the recipient of data is a company which has to comply with this directive, these guarantees result from the directive[6].

[4] This is decided by the European Commission.

[5] However, an additional prerequisite for the transfer is a legal basis.

[6] However, an additional prerequisite for the transfer is a legal basis.

8.2 Disclosure of data transferred to a third country within this third country or to another third country

The disclosure of transferred personal data to a body within this third country or to another third country shall only be allowed, with due regard to item 5), if this third country/the receiving body ensures an adequate level of data protection or if one of the conditions referred to in item 8.1 is fulfilled.[7] In the case of an RI group company unit having undertaken to comply with this directive, this does not have to be verified; otherwise – unless one of the conditions referred to in item 8.1 is fulfilled – an adequate level of data protection shall be ensured, if necessary by obliging the recipient to comply with the principles of this directive. In any case the RI group company unit in the EEA which has disclosed the data shall be informed of this.

9 Special categories of personal data

The transfer and subsequent processing and use of special categories of personal data, i.e. details on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, shall generally be prohibited. If such processing is required nevertheless, explicit consent shall be required from the data subject unless

- the data subject is incapable of giving his/her consent; or
- the data subject has made public the data concerned; or
- the transfer and subsequent processing and use is necessary for the establishment, exercise or defence of legal claims (weighing of interests!).

This shall include data which has been collected in the third country.

10 Direct marketing/market and public opinion research

If personal data are processed or used for the purpose of direct marketing/market or public opinion research, the data subject shall be entitled to object to this use of data relating to him/her at any time.[8] In this case the data shall be blocked for this purpose.

11 Automated individual decisions

If personal data are transferred and possibly processed with the aim of taking an automated individual decision, the legitimate interests of the data subject shall be protected by appropriate measures. Decisions which produce negative legal effects concerning the client or significantly affect him/her may not be based solely on an automated individual decision which serves to evaluate certain personal aspects. Exceptions to this shall be permitted only if the interests of the data subject are protected through information on the rationale of the decision and the possibility to comment on it. In the case of comments by the data subject, the controlling body shall be obliged to review its decision.

---

[7] However, an additional prerequisite for the transfer is a legal basis.

[8] To the extent provided by national law, the data subject is to be informed about his/her right of objection and the controlling body.

12 Procedural questions

12.1Implementation in the company

By undertaking to adhere to the above-mentioned principles, the RI group company units as competent recipients shall ensure that these principles are adhered to with respect to third parties (e.g. clients, intermediaries etc.).

In this respect, the senior staff of individual companies shall ensure the implementation of this directive, which includes above all instruction of staff members to this effect. If any training is needed, staff members shall approach the Data Protection Officer of the RI group[9]. Instruction shall include pointing out that any violation of these principles of data protection may possibly have consequences under criminal law, civil liability law or labour law.

12.2Questions and complaints

In the case of questions and complaints, data subjects may at any time approach the Data Protection Officer of the RI group[10] or his/her local representative and/or the competent supervisory authority. Recipients in third countries and the Data Protection Officer of the RI group[11] in the EU shall cooperate with the supervisory authority of the state in which the transferring body has its head office and respect its statements for all enquiries of this authority. Also the transferring body in the EEA shall be entitled to verify the data processing with the receiving body in individual cases. It will enforce rights which have been ascertained and support any data subjects who have sustained a loss through non-compliance with the obligation resulting from this directive in enforcing their rights with respect to the controlling body in the third country.

Data subjects may exercise their rights free of charge in out-of-court procedures.

13 Publicity

This company directive shall be made available to data subjects in an appropriate way, e.g. via the Internet.

14 Data Protection Officer of the Munich Re reinsurance group (RI group)

A Data Protection Officer for the Munich Re reinsurance group shall be appointed[12] who, together with the Group auditor or the auditors of the respective RI group company units, supervises compliance with national[13] and international data protection rules and these

[9] Please contact the RDPA (Regional Data Protection Adviser) or the Data Protection Officer of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München.

[10] The Data Protection Officer of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München.

[11] The Data Protection Officer of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München.

[12] The Data Protection Officer of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München.

[13] The national data protection regulations are examined by the local business units themselves.

guidelines. In this respect, he/she shall be supported by local representatives[14] who are responsible on his/her behalf for ensuring data protection in the company concerned as controlling body and inform him/her of complaints; they shall respect his/her statements. The senior staff members concerned shall support them in their activities.

All staff members may at any time approach the Data Protection Officer of the RI group[15] with questions, suggestions or complaints, which shall be treated confidentially.

The Data Protection Officer of the RI group[16] is currently Dr. Wolfgang Mörlein; you can reach him as follows: Datenschutz@munichre.com

[14] RDPAs (Regional Data Protection Advisers).

[15] The Data Protection Officer of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München.

[16] The Data Protection Officer of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München.

Annex 1
Munich Re reinsurance group directive on third-country data transfer

If personal data are processed **or used** in an automated way, **the internal organization shall be designed in such a way as to ensure that it meets the special requirements of data protection. In particular**, measures shall be taken which, depending on the type of personal data **or categories of data** to be protected, are appropriate

1. to refuse unauthorized persons **admittance** to data processing equipment used for processing **or using** personal data **(control of admittance)**,

2. to prevent any use of data processing systems by unauthorized persons **(control of admission)**,

3. to ensure that persons authorized to use a data processing system may only access data which is subject to their access authorization **and that personal data may not be read, copied, altered or removed in an unauthorized way when being processed or used and after being recorded** (control of access),

4. to **ensure** that personal data **may not be read, copied, altered or removed in an unauthorized way** during their **electronic transfer** or during their transport or their **recording on data media and that it may be checked and established in which places any transfer of personal data by institutions for data transmission has been provided for (control of disclosure)**,

5. to ensure that it may subsequently be checked and established **whether and by whom** personal data has been input into data processing systems, **altered or removed** (control of input),

6. to ensure that personal data which is processed on behalf of another body may only be processed in accordance with the instructions given by the principal (control of order),

7. **to ensure that personal data are protected against fortuitous destruction or loss (control of availability),**

8. **to ensure that data which has been collected for different purposes may be processed separately.**

Annex 2
Munich Re reinsurance group directive on third-country data transfer

Formal obligation to observe data secrecy

Mr./Ms.
.....
(Name, employee number)

is herewith obliged to observe data secrecy.

The employee is advised that it is prohibited to illicitly process or use any protected personal data for any other purpose than that relating to the legitimate fulfilment of the relevant tasks and that these obligations continue even after the activity has been terminated.

The obligation covers the following items:

- Any data or routines may only be stored, processed or printed out in the way ordered by bodies authorized to take decisions.
- Data, routines or other information may not be duplicated for any purpose other than the relevant commercial purpose.
- It is prohibited to falsify data or routines, to produce false data or routines or to deliberately use false or falsified data or routines.
- Only data necessary for the actual fulfilment of tasks may be retrieved.
- Disclosure of personal data to third parties is only allowed if the recipient is granted a right of access by virtue of a legal provision.
- Documents including personal data have to be stored in a way that protects them against any access by third parties.

Existing regulations on the handling or protection of personal data (e.g. with respect to protection by passwords) have to be complied with. For the protection of personal data, these have to be handled with due care within the scope of the task assigned; any deficiencies noticed have to be reported.

The employee is advised that any infringement of data secrecy may entail imprisonment or a fine under the relevant legal provisions. Any violation of data secrecy will in most cases represent simultaneously an infringement of professional secrecy, which will entail measures taken under labour law even including termination without notice.

The receipt and acknowledgement of this formal obligation shall be confirmed by returning a signed copy to the Data Protection Officer (the returned copy will be added to the employee's personnel file).

.....
(Date)

.....
(Signature of the employee)

Annex 3
Munich Re reinsurance group directive on third-country data transfer

The European Economic Area (EEA) is made up of the countries of the European Union (EU) and the Member States of the European Free Trade Association (EFTA) excluding Switzerland.

Thus, the following countries belong to the EEA:

EU Member States

Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
United Kingdom

EFTA Member States

Iceland
Liechtenstein
Norway