Data Protection Overview

Data Protection Overview

Scope of Presentation

- Highlights of MR Group Directive on 3rd Country Data Transfer
- Responsibilities and expectations
- Action items

- Remember “Legitimate Business Reason”

Data Protection Overview

Munich Re Group Directive on 3rd Country Data Transfer

- Contains legal requirements for protection of "Personal Data"
  - Any information relating to and identifying a person (e.g., name, address, home phone #, social security #, employee ID #, etc.), is included - it is not only private personal data
- Created by German Association of Insurers (Munich Re is member)
- German Supervisory Authorities approved it in 2002

Data Protection Overview

Munich Re Group Directive on 3rd Country Data Transfer

- Describes a framework for establishing an adequate level of data protection within MRG
  - System controls (e.g., security, tracking, data integrity, etc.)
    - Does not specify what level of system controls is adequate (becomes subjective, depending on the nature of the data, the purpose of processing etc.)
  - Education & awareness
  - Signoff from employees that they are aware and will comply (called “Formal Obligation”)

Data Protection Overview

Munich Re Group Directive on 3rd Country Data Transfer

- Applies to Personal Data that is being **processed/ stored** by a MRG Business Unit (data controller) in an European Economic Area (EEA) state and is **transferred** to BUs in 3rd Countries
  - Includes system files or hardcopies
  - Transferring includes providing display access (MRWeb – Smart Directory, FS-RI, Claims)
  - Applies to European or non European Personal Data

Data Protection Overview

Munich Re Group Directive on 3rd Country Data Transfer

- Does not apply:
  - Transfer of Personal Data from a Cedent located in EEA to MR office (but Cedent might wish to agree such provisions)
  - Transfer of Personal Data within EEA member states

Data Protection Overview

Munich Re Group Directive on 3rd Country Data Transfer

- Indicates consent from data subject could be required, in particular if special categories of personal data (e.g. health data) are concerned, in general EEA-BU is responsible
- Directive requires that only authorized individuals can access Personal Data, and not for private reasons

Data Protection Overview

Compliance Checks at MR

- German Authorities could perform compliance review of MRM including compliance of Non-EEA-BUs with MRG-Directive
  - None performed yet or scheduled
- Internal & external auditors might review for compliance
- Data Protection Officer (DPO) might assess the MR local office compliance with Directive

Incidents

- Incident can be when Personal Data is deleted, changed, stolen, accessed by unauthorized parties, etc.
- RDPA must report incidents to DPO (may be reported to Board of Management.)

Data Protection Overview

Data Protection Officer (DPO)

- Dr. Wolfgang Mörlein
- Overall DP responsibility for MR Group since 2006, for MRM since 1997
- Regional Data Protection Advisers report to him
- Point of contact for incidents
- Very involved with the creation of the “Munich Re Group Directive on 3rd Country Data Transfer”

Data Protection Overview

Regional Data Protection Adviser (RDPA)

- Lead the effort to ensure compliance
- Determine where compliance is needed
- Assist appropriate areas with establishment of action plans for evaluating and implementing compliance
- Address regional staff questions/incidents
- Report on compliance and non compliance to DPO
- Provide DPO with information about systems, training, contracts, Formal Obligations, etc.

Data Protection Overview

Local Data Protection Contact

- Local “eyes and ears”
- Contact person for the RDPA West (Rob Jemmett) and for the Group Data Protection Officer (Dr. Mörlein)
- Helps at local level for checking laws, contracts, uses of information which falls under the Directive
- Introduces the RDPA to the person (internal or external) who is responsible for issues
- Needs no special qualifications
- No restriction in regard to the business function of the local contact
- Not necessary to have the same skills as the RDPA

Data Protection Overview

Action Items

- RDPA discuss initiative and obtain feedback
- Identify and document what Personal Data is accessed which originates out of an MRG Office from the EEA
- Complete checklist provided by DPO

Data Protection Overview

Action Items

- Identify systems/files located outside of Europe (e.g., in Sao Paulo, Buenos Aires, Santiago) that store Personal Data that originates from an MRG office in Europe
    - Complete checklist provided by DPO
    - Ensure these systems are in compliance (i.e., system & physical controls)
- Provide training and awareness to staff
- Begin to make Directive known

Data Protection Overview

Action Items

- Ensure contracts with externals contain appropriate provisions that describe data protection obligations
    - Identify applicable contracts and update if feasible
    - Create templates for new contacts & implement going forward

Data Protection Overview

Action Items

- Obtain and maintain “Formal Obligations”
- Establish wording and process/method for obtaining signoff
    - Obtain signoff from existing employees
    - Establish approach for new employees
- Provide annual report to DPO at the end of the year that describes status of Data Protection initiative