RUOSS VÖGELE PARTNER
RECHTSANWÄLTE ATTORNEYS AT LAW
RVP

RUOSS VÖGELE PARTNER | KREUZSTRASSE 54 | CH-8032 ZÜRICH
TELEFON +41 44 250 43 00 | FAX +41 44 250 43 10 | info@rvpartner.ch | www.rvpartner.ch

RVP Bulletin

Regulating Data Protection in Multinational Companies (Overview)

Dr. Alois Rimle, LL.M.
rimle@rvpartner.ch

Zurich, February 2014, No. 1

Contents

Processing of Personal Data in Multinational Companies

Description of data processing

One must first establish the relevant facts before being able to identify and implement the requirements under applicable data protection law in a multination-

al company. It generally depends on the business activities of the enterprise which types of personal data are being processed and in which manner.

The data processing operations in a multinational company must be described in an appropriate way. The description mainly includes the following elements:

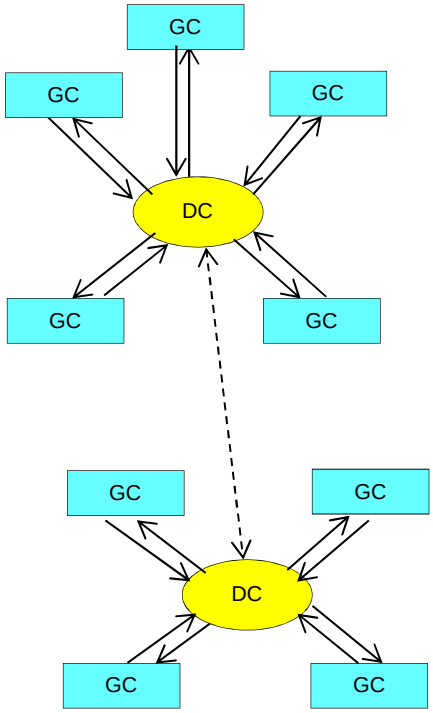
- Group chart with indication of countries;
- Business functions and organization;
- IT infrastructure (data centers and server locations);
- Data processing operations;
- Types of data subjects and personal data;
- Data flow with data entry and data access;
- Outsourcing of data processing (cloud).

IT infrastructure and applications

In the context of electronic data processing in a multinational company one may distinguish between data center (IT infrastructure), platform (applications) and software (software applications):

- *Data Center:* Multinational companies regularly operate regional or global data centers. These data centers comprise servers that allow the group companies to save their data or applications. The IT infrastructure concerns the network, access to the network, hardware etc. Data centers regularly include operative servers at one location and back-up servers at another geographically separate location. They further include a security deployment for important non-foreseeable contingencies.
- *Platform:* A platform (application) is developed and made available for data processing operations in the data center.
- *Software:* There must be application software that allows the management of the data by means of the platform.

A multinational company generally operates (besides local servers) one or several data centers. The group companies will generally be allocated to a specific regional or global data center. There is possibly limited exchange of data between the different data centers. Data transfers over the data centers of a multinational company may be illustrated in a simplified way as follows:



Documentation and Actualization

The description of the processing of personal data in a multinational company must be documented. In particular, there should be an inventory of the various data processing operations. Also lists of relevant data files need to be prepared for those group companies that are subject to respective reporting obligations under local data protection law.

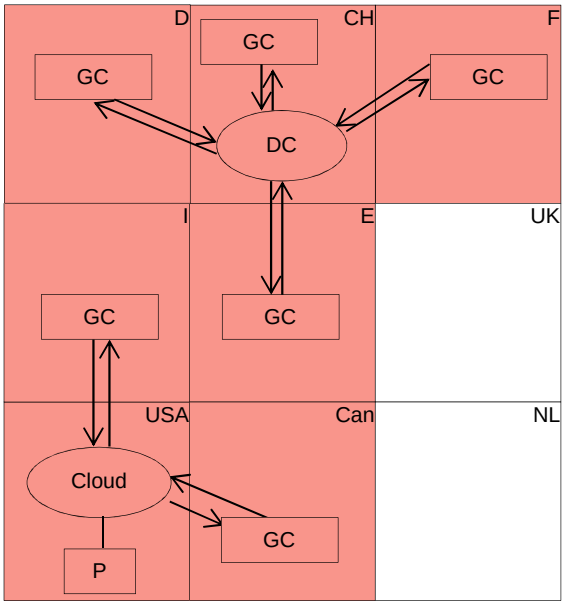
The data processing operations in a multinational company are constantly changing. Existing processing operations are changed and new processing operations introduced. Therefore, the existing documentation on internal data transfers must regularly be updated in a multinational company.

Applicable data protection laws

Data protection law is mainly national law. The national data protection laws that are applicable to the processing of personal data in a multinational com-

pany are generally determined based on where personal data is processed. Generally, data processing takes place where group companies have their business activities and where data centers are located. Whether a particular data protection act is applicable must be determined based on the scope of such act.

A multinational company has its business activities in many countries and must therefore observe various data protection laws. This may be illustrated in a simplified way as follows:



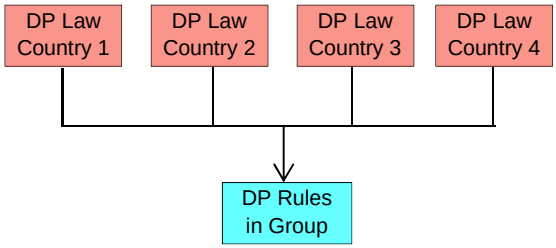
The statutory provisions in national data protection laws are mainly of a private, administrative or criminal law nature. Their application to the group-wide processing of personal data is different depending on their qualification:

- *Private-law provisions:* The private-law provisions (in particular processing principles) are generally alike in different countries. If a high data protection standard is applied based on one country's private law provisions it may generally be assumed that such standard also complies with the statutory requirements in other relevant countries. Exceptionally, there are particular private-law requirements in certain countries that need to be separately addressed under the relevant local laws. Such requirements exist for example for Germany in the area of data transfers or for Spain in the area of data security.
- *Administrative-law provisions:* The administrative-law provisions (in particular, reporting obligations) must be determined and complied with separately in each relevant country.
- *Criminal-law provisions:* The criminal-law provisions in data protection acts are generally connected to a breach of administrative-law provisions. If applicable, they must be observed separately in each concerned country. However, if they are connected to a breach of private-law provisions criminal liability may regularly be avoided by implementing a high data protection standard.

Implementation of law in a multinational company

It is practically not possible that multinational companies directly apply national data protection laws to their intragroup processing of personal data. Also data protection laws generally require that statutory provisions be implemented by means of intragroup rules stated in guidelines, policies and contracts.

The implementation of applicable data protection laws in multinational companies may be illustrated in a simplified way as follows:



Privacy impact assessment

If a new system or data processing operation with higher data protection risks is intended to be implemented in a multinational company a privacy impact assessment must first be performed. The assessment serves the purpose of warning of data protection risks and allows early in the process to identify those items of a project that are critical from a data protection law perspective. There are relevant evaluation forms available in Switzerland as well as in the EU. Based on the results of the impact assessment, the project may be structured in a way that takes requirements under applicable data protection law into consideration.

Measures under Data Protection Law

Limited collection of personal data

Based on the principle of reasonable data processing, an enterprise must generally only collect such personal data that is actually needed for its own business operations. It may not collect personal data as a reserve. An enterprise that systematically collects unnecessary personal data generally acts contrary to data protection law.

In this context it is recommended for enterprises to consciously manage their collection of personal data. For example, it should be defined and documented in the HR department which types of information from which categories of employees may or may not be collected. The same applies to the collection of customer data. Furthermore, procedures should be established for the destruction or deletion of personal data that are not needed any longer (or of personal data wrongly collected as a reserve).

In particular, the collection of sensitive personal data and personality profiles should be avoided or restricted to the extent possible. The processing of such information is subject to additional restrictions and requirements (e.g. consent requirement) under the data protection laws of countries with adequate data protection.

Handling of private information

Enterprises may generally not process private information of employees or customers. Nevertheless, it is practically not possible to entirely avoid the processing of private data in an enterprise. For example, employees may send or receive private e-mails that may be stored on the enterprise's e-mail server. Employees may store private content on their personal computer. Customers may place private information on the website of the enterprise.

Since enterprises must avoid the processing of private information to the extent possible, it seems to be advisable to develop a concept how to deal with private information. In particular, the following restrictions should be observed: The retention of private information should be limited to the extent possible. Furthermore, stored private information may only to a very limited extent be included in monitoring actions (e.g. e-mail or internet monitoring) of the enterprise (see guidance issued by data protection authorities in relevant countries). Finally, data subjects are generally entitled to ask for the deletion of their private information and may enforce their right against the enterprise under applicable data protection law.

Conversion into non-personal data

Data protection law requirements only apply if personal data is processed. If data is processed that is not personal data, then there is no need to observe any requirements under data protection law. Personal data is defined in Swiss data protection law as "all information relating to an identified or identifiable person" (Art. 3 para. 1 lit. a DPA) or in the EU Data Protection Directive as "any information relating to an identified or identifiable natural person" (Art. 2 lit. a EU Data Protection Directive).

The Swiss Supreme Court has stated the following in this context: „A person is identifiable if he or she may be determined based on additional information. However, determinability requires more than just the theoretical possibility of identification. If the expenses are so high that it may not be expected based on general experience of life that an interested person would accept them, there will be no determinability. The question must be answered based on the circumstances of a particular case and thereby also taken into consideration the feasibility of technology, for example the search tools in the internet. However, it is not only relevant what expenses are objectively incurred when allocating specific information to a person but also what interest the processor of the data or a third party has in the identification." (SCD 136 II 508, 514). "Whether information may be linked to a person based on additional indications, i.e. the information relates to an identifiable person (Art. 3 lit. a DPA), must be determined from the perspective of the respective keeper of the information." (SCD 136 II 508, 515).

If one assumes that there are similar rules applicable to the determinability of a person in other countries, it will be possible for multinational companies to convert to some extent personal data into non-personal

data for the purpose of specific processing steps or storage and thereby avoid the application of data protection law. For example, if anonymized or pseudonymized data is transferred to a service provider abroad (without authority for onwards transfers) and the service provider is unable to arrange for re-identification, then the data is not personal data from his perspective for lack of relation to a person. If applicable, the requirements under data protection law for cross-border data transfers to countries not providing adequate data protection do not need to be observed. The same may apply if electronic personal data (i.e. programs) is "split" or possibly if personal data is fully encrypted.

More is better than less

It is not quite right to say that data processing in a multinational company as a whole is either compliant or not compliant with applicable data protection law in my opinion. It is more appropriate to say that data processing in a multinational company as a whole is more or less compliant, however, never 100% compliant with applicable data protection law. Therefore, the processing of personal data in a multinational company may and should periodically be reviewed and adapted or improved based on applicable data protection law.

Risk-based approach

Some processing systems in a multinational company may include a lot of personal data (e.g. HR systems), others may hardly include personal data. Furthermore, personal data is not equal to personal data. For example, the unlawful disclosure of sensitive personal data is more severe than the unlawful disclosure of simple personal data from the perspective of personal rights.

Therefore, it is important to identify those processing operations in a multinational company that include a lot of or delicate personal data, in particular, sensitive personal data or personality profiles. Data protection measures should at first focus on the respective processing operations.

Security and storage in data centers

The setting-up of data centers in a multinational company is a good idea not only for efficiency and cost reasons. Also they generally allow the implementation of a higher level of data security than it would be possible in the case of local servers. Therefore, data processing in regional and global data centers is welcome also from the perspective of data protection law.

Data centers do not only serve the purpose of data storage but also electronic storage of documents. They do not only include structured databases but also systems for the storage of documents and e-mails (document and e-mail repositories). The electronic storage of documents may be structured in such a way that statutory safekeeping requirements in the concerned countries are fully met or met to a large extent so that all or most types of documents no longer need to be kept in paper form.

The electronic storage of data and documents is sometimes aligned with possible future disclosure requirements. For example, the storage of e-mails may specifically be set up in view of future group-wide data disclosure in the context of pre-trial discovery in particular in the USA.

It should finally be mentioned in this context that the storage of data and documents in regional or global data centers of a multinational company may be subject to supervisory law requirements and restrictions if regulated business activities are concerned. If applicable, data centers may be considered as cases of IT outsourcing under supervisory law that need to be reported to the regulators or even approved by them in the relevant countries.

Data protection compliant products

Applications must be developed in due consideration of data protection law. Under Swiss data protection law it is generally possible to certify products, the actual purpose of which is data processing and products the use of which leads to the collection of personal data (Art. 5 DPCO). In the course of certification the product intrinsic provision of various data protection aspects is assessed.

Standard transparency

Data subjects must know or be able to realize that their personal data is processed by a particular enterprise so that they are in a position to exercise their

rights. As a result, an enterprise will regularly need to inform the data subjects about the collection and processing of their data under applicable data protection law. This principle applies not only under Swiss but also under other data protection laws.

Enterprises should inform their employees, customers and suppliers about the processing of their data, if legally required, as a matter of standard procedure and preferably on a group level. The information may be provided by means of contractual clauses, separate notices, website notices or by other means.

Identification of consent cases

The consent can be considered as a problematic justification of the processing of personal data: First, the requirements for a valid consent under data protection law are high. If the consent is used incorrectly it may not be considered as appropriate basis for data processing. Second, the consent will not be able to justify data processing if it is granted in the context of a clear imbalance between data responsible person and data subject (e.g. cases of consent in employer-employee relationship). Third, the consent is an unstable justification of data processing, as it may be withdrawn at any time.

The consent is one of several possible justifications of the processing of personal data under data protection law. In a multinational company the consent should be used only if there is no other justification of any necessary data processing operation. In particular, the consent of employees and customers is generally not suitable for standard processing operations where there is no processing alternative in the case of consent withdrawal. However, specific and one-time data processing events may be justified based on consent (e.g. consent of employee to psychological test in a promotion or hiring procedure).

It appears to be useful in a multinational company to investigate the various justifications of data processing operations under data protection law and identify those cases where the consent of the data subject is required. As regards these cases, a standard written consent declaration may be drafted and used in a way that is valid under data protection law.

Data Protection Governance

Effective implementation in multinational companies

Multinational companies must take practical measures in order to effectively implement requirements under data protection law. In particular, the following measures appear to be important: entering into data transfer agreements, issuance of guidelines and policies, appointment of responsible persons, conducting data protection trainings, specification of data protection procedures and compliance measures. Data protection should mainly be organized centrally in a multinational company, in particular because group-wide data processing operations are subject at the same time to several data protection laws with comparable requirements.

Responsible persons

It appears necessary to appoint a person responsible for data protection and a person responsible for data security on a group level. These functions may be merged and combined with other functions depending on the circumstances of the particular case. The responsible persons should be granted considerable responsibilities in the areas of data protection and data security, as these areas mainly concern “technical” questions to be answered by Legal & Compliance or IT in a fast and flexible way and followed by efficient measures. Furthermore, on the level of the countries or group companies it may be required under applicable data protection law to appoint a local person responsible for data protection.

Data protection trainings

Employees of a multinational company whose tasks include the processing of personal data (e.g. HR personnel) must be trained in data protection law from time to time in order to be able to apply the existing group guidelines and processing policies in their areas of responsibility.

Data protection procedures

The following data protection procedures should generally be set up in multinational companies:

- Procedures to manage access, correction and deletion requests from data subjects;
- Procedures to handle internal complaints;
- Procedures for the effective management and reporting of security breaches;
- Procedures for the performance of privacy impact assessments in specific circumstances;
- Procedures for the performance of compliance measures.

Compliance

It should periodically be verified in multinational companies that existing data protection measures are sufficient to effectively implement the processing principles and other requirements under applicable data protection law. The responsible persons may carry out checks, and internal or external audits may be performed. This is how it can be ensured that data protection measures do not only exist on paper but are actually implemented.

Agreements for Intragroup Data Transfers

Contract requirement for data transfers

In a multinational company there are numerous transfers of personal data between group companies taking place over group-wide processing systems every day. Such data transfer operations generally require the entering into written data transfer agreements between the concerned group companies based on EU and Swiss data protection law.

A written data transfer agreement is usually necessary if personal data are transferred cross-border from an EU Member State or Switzerland to a country not providing adequate data protection. The transfer agreement is intended to ensure adequate data protection on the side of the data recipient. Appropriate standard contractual clauses are available in the EU and Switzerland. A written agreement is even necessary for data transfers within the EU or Switzerland if a company contracts processing operations to another company (contracting of data processing). These contract requirements also apply to intragroup data transfers of a multinational company.

The situation is different if a multinational company has implemented Binding Corporate Rules. If applicable, there will be a reduced and different need for binding contracts (see below).

Multilateral data transfer agreements

It would not be practical to enter into bilateral agreements between concerned group companies for all types of data transfers in a multinational company. Therefore, it is advisable to enter into one or few multilateral agreements instead of numerous bilateral agreements in a multinational company.

Multilateral agreements may be entered into on the level of the individual processing systems (e.g. HR database, business systems, e-mail server, etc.). This approach, however, will still require many multilateral agreements, at least in big multinational companies. It therefore appears sensible to draft one single agreement for all business-related data transfers. Such an agreement will certainly be extensive and include several appendices to cover the different business functions with their corresponding processing systems. However, it is still easier to handle one single complex agreement than a multitude of bilateral or system-related multilateral agreements. Besides such a comprehensive business-related agreement, one will generally only need another multilateral agreement for HR-related transfers.

„Ring fencing“ on a low level of protection

From the perspective of Swiss and EU data protection law there are on the one hand countries providing adequate data protection (EU Member States, Switzerland, certain other countries) and on the other hand countries not providing adequate data protection. In situations where the processing of personal data is restricted to countries not providing adequate data protection, there is no need to apply higher level data protection law requirements applicable in countries providing adequate data protection. Therefore, it is generally possible for multinational companies to operate the intragroup processing of personal data on different protection levels. For example, data processing in Switzerland must be operated on a high level, whereas data processing in the USA may be

operated on a lower level. It is another question whether this is desirable. Many multinational companies rather want to consistently implement a high data protection standard across the entire group and communicate such standard to their customers and the public.

The processing of personal data on a lower level is only admissible in a multinational company as long as it is restricted to countries not providing adequate data protection. It thereby still remains possible for group companies in countries not providing adequate data protection (e.g. USA) to transfer their personal data to a centralized group server in a country providing adequate data protection (e.g. Switzerland) and store the data and access it online on the system abroad. As long as only personal data which has been transferred before is processed online by employees from the original countries, the relevant group companies do not generally need to be committed to apply a higher data protection level under applicable data protection law in my opinion. However, the situation is different for personal data that was not transferred before but rather newly or additionally created in the course of data processing in the group system. The processing of such data will generally be subject to the higher data protection level ("infection by higher data protection standard").

Group Guidelines and Policies

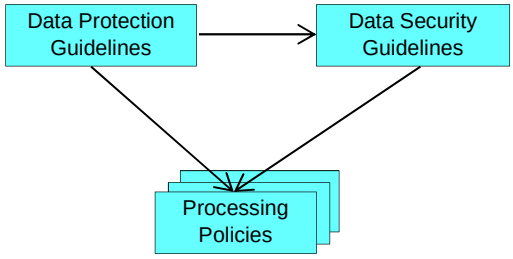
Regulation architecture in multinational companies

In the interest of effective data protection in a multinational company it is essential that the responsible employees are appropriately instructed how to process personal data in compliance with the law. This does not only concern employees in countries providing adequate data protection, but also employees in countries not providing adequate data protection. The employer group companies in such countries have a contractual obligation to apply an adequate level of data protection based on the intragroup data transfer agreements (see above).

One may ask the question how employees who process personal data as part of their tasks can best be informed and instructed in a multinational company. Data protection information and instructions to employees are generally provided by means of guidelines and policies.

Data protection and data security guidelines must first be issued by the competent body on a group level. Group guidelines are indeed necessary, however, do not generally help the individual employee when dealing in practice with personal data in his or her field of work. For example, if the group data protection guidelines state that personal data must be processed based on the principle of reasonable data processing, the individual employee will often not know how to apply such processing principle in the case at hand. Therefore, the group data protection guidelines generally need to be implemented with respect to particular data processing operations by means of appropriate processing policies (e.g. HR processing policy).

The architecture of data protection guidelines and policies in a multinational company may be illustrated in a simplified way as follows:



The guidelines and processing policies in a multinational company are mainly addressed to employees who process personal data. Accordingly, they must (other than data transfer agreements) be drafted in a simple and understandable way.

Data protection guidelines on a group level

The group data protection guidelines merely include a framework under data protection law. They will (among others) cover the processing principles and aspects of data protection governance. As regards detailed regulation on a group level, the group data protection guidelines may refer to separate guide-

lines and thereby delegate authority (e.g. regulation of data processing procedures).

Data security guidelines on a group level

IT specific risks must be dealt with based on effective risk management. The risk management must be implemented through clearly defined IT governance and an aligned IT security strategy. The IT governance comprises the steering and monitoring of risks as well as the specification of responsibilities in information technology. The IT security strategy determines the security standards and security goals.

The contents of IT governance and information security are specified in internationally recognized frameworks (self-regulating standards, e.g. ISO 2700X). Based on the contents of these international frameworks and the statutory requirements in the concerned countries, information security guidelines must be issued in order to specify the IT governance, IT security strategy and their implementation. Finally, it is for example also necessary to regulate reporting and adaptation to the changed circumstance.

Processing policies

In a multinational company there are regularly many different data processing operations and in each case one may need to deal with specific issues under data protection law. Therefore, it is necessary to issue rules for important data processing operations under data protection law. Rules are not only necessary for HR data processing (e.g. hiring process, internet and e-mail surveillance, video and GPS surveillance etc.). Rather, each important processing system with specific purpose may require particular guidance as to how to process personal data in such system. Accordingly, for example Swiss data protection law includes a general duty to issue a processing policy for each automated data file where personal data are regularly disclosed to third parties or where sensitive personal data or personality profiles are regularly processed (Art. 11 para. 1 DPO).

It makes sense for several reasons in my opinion to delegate the authority to issue specific processing policies to the responsible person for data protection in a multinational company: The responsible person for data protection is technically able to decide on the need and content of processing policies. Also he or she will be able to react to the continuous transformation of the data processing set-up in a multinational company and, if necessary, update existing processing policies without delay. This is in the interest of effective data protection in a multinational company.

Binding Corporate Rules

BCRs as approved overall data protection concept

The use of Binding Corporate Rules (BCRs) as legal basis for cross-border data transfers within a multinational company requires under EU law that the data controllers in the group have taken appropriate protection measures. Based on such measures and their documentation, the intragroup data transfers can be approved by means of a particular EU procedure under the responsibility of a lead regulator. BCRs include internal measures for the implementation of the processing principles in the multinational company (e.g. appointment of responsible person, specification of procedures, conducting trainings, issuance of guidelines). These group-wide internal measures eventually serve the implementation of the contractual guarantee of adequate data protection for cross-border data transfers to countries not provided adequate data protection.

The approval of BCRs is also available for multinational companies with head office in Switzerland and subsidiaries in the EU. Swiss multinational companies can generally initiate the approval procedure before the data protection authority of an EU Member State where they have business activities. Once the BCRs have been approved in the EU, they must also be communicated to the Swiss Federal Data Protection and Information Commissioner (Art. 6 para. 2 lit. g and para. 3 DPA; Art. 6 para. 1 DPO).

Contents of BCRs

The BCRs (understood in a broader sense) represent an overall concept for the regulation of data protection in a multinational company and include all ap-

proved and documented measures. In particular, they include the following types of documents:

- Approval request with explanations and descriptions of the processing systems and data flows;
- BCRs (understood in a narrower sense) as higher data protection guidelines, possibly with appendices;
- Guidelines and policies that in particular also describe data protection procedures;
- Required intragroup transfer agreements;
- Information documents (transparency);
- Specific requirements based on national data protection laws (e.g. reporting duties).

Approved BCRs or independent protection measures

A multinational company does not necessarily need to get BCRs approved in order to ensure general compliance of intragroup data protection measures with the law. A multinational company may also independently ensure general compliance with the law without governmental approval by means of entering into multilateral transfer agreements and in addition issuing guidelines and policies and implement them. It follows that multinational companies may choose between governmentally approved BCRs and independently implemented data protection measures. Both approaches require comparable documents. However, the contractual requirements for BCRs are partly different and less extensive than for independently implemented data protection measures.

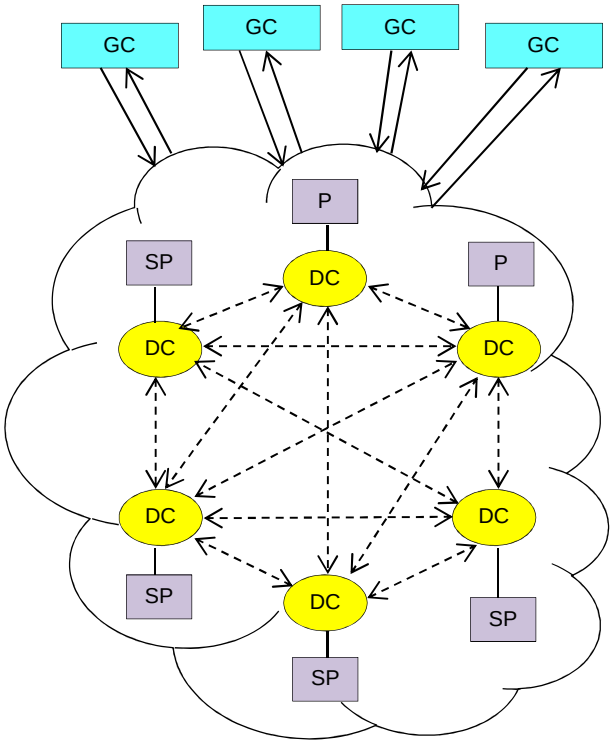
Cloud Computing

External data processing

It appears sensible for cost reasons that a multinational company has part of its data processing operations being performed by a specialized service provider in a cloud. What is meant here by a cloud is a so-called “public cloud” where the infrastructure is fully operated and determined by an external cloud provider. In particular, the cloud client has no bearing on the locations of the servers.

Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. The service may merely consist of the infrastructure where the cloud provider makes a server available in the cloud on which the cloud clients may then store their data and applications (infrastructure as a Service (IaaS)). Furthermore, the cloud provider may develop an application and make it available to the users in the cloud for the purpose of data management (Platform as a Service (PaaS)). Finally, the cloud provider may also take over the management of the data by means of appropriate software so that the cloud client is merely a consumer in the cloud to whom functionality is made available in order to be able to process data there (Software as a Service (SaaS)).

Cloud computing services may entail the involvement of a number of contracted parties who act as processors. It is also common for processors to subcontract additional sub-processors which then gain access to personal data. As a consequence, there may be numerous data transfers between servers and data centers, respectively, of processors and sub-processors in the cloud. The processing of personal data on behalf of group companies in a cloud may be illustrated in a simplified way as follows:



Risk and risk analysis

The data protection risks in the context of cloud computing are mainly a lack of control over personal data and insufficient information with regard to how, where and by whom the data is being processed/sub-processed.

The relationship between cloud client and cloud provider generally qualifies as controller-processor relationship under data protection law. The enterprise which transfers personal data to a cloud will be responsible for the compliance with data protection law. It must therefore choose a cloud provider that guarantees compliance with applicable data protection law and ensure that the legal requirements are actually implemented. Such responsibility does not only concern data security aspects but also various duties under data protection law (e.g. compliance with purpose limitation, principle of reasonable data processing, transparency, etc.).

It follows that an enterprise must perform a risk analysis under data protection law before mandating a cloud provider. It needs to consider which applications and data it wants to keep at its own location and which applications and data it wants to transfer to the cloud and, if applicable, which type of cloud. As regards the cloud providers, one may in particular distinguish between cloud providers who guarantee data processing on the territory of Switzerland or the EU and cloud providers who do not provide any such guarantee. One may possibly also wish to consider the risk of data surveillance in the event of a US provider and server locations in the USA, respectively.

Agreements and Processor BCRs for the cloud

Cloud computing is regularly based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data center at 3 pm and at 6 pm in another data center on the other side of the world. In this context, the traditional legal instruments to regulate data transfers to countries not providing adequate data protection have limits.

One possibility of regulation consists of using standard clauses in agreements between the enterprise and the cloud provider established in a country not providing adequate data protection and, if necessary, amending the standard clauses (in which case the clauses are no longer "standard"). If the cloud provider is established in a country providing adequate data protection, the situation might be more complex since the model clauses, in general, do not apply then. As regards the contractual relationship between the processor in a country not providing adequate data protection and the sub-processor, a written agreement which imposes the same obligations on the sub-processor as are imposed on the processor in the model clauses should be entered into.

An alternative possibility of regulation in the EU consists of the Processor BCRs that were developed by the Article 29 Data Protection Working Party in 2012 and 2013. They allow the transfer within the group of the cloud provider (i.e. to sub-processors) for the benefit of the controllers without requiring the signature of contracts between processor and sub-processors per client. The contents of the Processor BCRs of a processor group must be pre-approved by the concerned data protection authorities in the EU. The approved guidelines can then form an appendix to the services agreement between the cloud provider and the relevant enterprise (client).

Abbreviations

BCRs:	Binding Corporate Rules
DC:	Data Center
DP:	Data protection
DPA:	Swiss Data Protection Act of 1992
DPCO:	Swiss Data Protection Certification Ordinance of 2007
DPO:	Swiss Data Protection Ordinance of 1993
EU:	European Union
GC:	Group company
HR:	Human Resources
P:	Processor
Processor BCRs:	Processor Binding Corporate Rules
SCD:	Swiss Supreme Court Decision
SP:	Sub-Processor

Auf www.rvpartner.ch verfügbare Bulletins und Broschüren in PDF-Form

2013

- Wettbewerbsabreden und Marktbeherrschung unter besonderer Berücksichtigung des schweizerischen Versicherungsmarktes (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Geschäftsraummiete
  Chasper Kamer, LL. M.
- Aufsichtsrechtliche Optimierung in der unabhängigen Vermögensverwaltung (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M
- Verantwortlichkeit und Haftung des Verwaltungsrats (eine Übersicht)
  (RVP)
- Umstrukturierungen im Versicherungskonzern (eine Übersicht)
  Dr. Alois Rimle, LL.M.
- Der Vorsorgeauftrag – Delegieren Sie Ihre Sorge(n)
  Bigna Grauer

2012

- Entwicklungen im Unternehmens- Datenschutzrecht der Schweiz und der EU im Jahr 2011
  Dr. Alois Rimle, LL.M.

2011

- Entwicklungen im schweizerischen Versicherungsrecht 2011/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im schweizerischen Transaktionsrecht 2011/1
  (RVP)
- Vermeidung der Regulierung von Private Equity-Investitionen in der Schweiz (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.; Alfred Gilgen, LL.M., N.Y. BAR
- Durchsetzung von Geldforderungen nach der neuen ZPO
  Dr. Alois Rimle, LL.M.

2010

- Der Aktionärsbindungsvertrag
  Chasper Kamer, LL.M.
- Entwicklungen im schweizerischen Transaktionsrecht 2010/1 (Deutsch und Englisch)
  (RVP)
- Entwicklungen im Unternehmens-Daten-schutzrecht der Schweiz und der EU 1/2010
  Dr. Alois Rimle, LL.M.
- Entwicklungen im schweizerischen Banken- und Kapitalmarktrecht 2010/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im schweizerischen Versicherungsrecht 2010/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Rechtliche Rahmenbedingungen der Unternehmenssanierung
  (RVP)

2009

- Entwicklungen im schweizerischen Transaktionsrecht 2009/2 (Deutsch und Englisch)
  (RVP)
- Überstunden und Überzeit
  Dr. Franziska Buob
- Entwicklungen im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2009/2 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU 2009/2
- Unternehmensleitung in Krisenzeiten
  Worauf es zu achten gilt
  Dr. Franziska Buob
- Entwicklungen im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2009/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU 2009/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im schweizerischen Transaktionsrecht 2009/1
  (RVP)

2008

- Revision des Revisionsrechtes: Eine Übersicht über die wichtigsten Neuerungen
  Sara Sager
- Entwicklung im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2008/2 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Vom Prozessieren
  Dr. Franziska Buob
- Liegenschaften im Erbgang: Häufige Tücken und Fallen (Teil I: Nachlassplanung)
  Pio R. Ruoss
- Outsourcing
  Dr. Marc M. Strolz
- IP IT Outsourcing
  Pascale Gola, LL.M.
- Entwicklung im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2008/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.

2007

- Aktuelles aus dem Bereich des Immaterialgüter- und Firmenrechts
  Dr. Martina Altenpohl
- Die „kleine Aktienrechtsreform“ und Neuerungen im Recht der GmbH
  Chasper Kamer, LL.M.
- Swiss Insurance Law Update 2007/1
  Dr. Alois Rimle, LL.M.
- Privatbestechung (Art. 4a UWG)
  Dr. Reto T. Ruoss
- Neue Phase der Freizügigkeit für EU/EFTA-Bürger, deren Familienangehörige und Erbringer von Dienstleistungen in der Schweiz
  Alfred Gilgen, LL.M.
- Revidiertes Datenschutzrecht für Unternehmen in der Schweiz
  Dr. Alois Rimle, LL.M.
- Aktuelles aus dem Bereich des Wettbewerbs- und Immaterialgüterrechts
  Chasper Kamer, LL.M.
- Actions Required under New Swiss Collective Investment Schemes Act
  Dr. Alois Rimle, LL.M.

2006

- Dokumenten- und Datenaufbewahrung im schweizerischen Unternehmen
  Dr. Alois Rimle, LL.M.
- Schweizerische Versicherungs- und Vermittleraufsicht
  Dr. Alois Rimle, LL.M.