ASSOCIATION OF EUROPEAN BUSINESSES
IN THE RUSSIAN FEDERATION

Round Table organized by the AEB IT-Telecom Committee

"Information Security & Modern IT-Solutions for Information protection "

June 3, 2010
AEB Premises, Moscow

Customs Union of Russia, Kazakhstan and Belarus

June 2010

PricewaterhouseCoopers

Customs Union: Recent developments

- The process of creation of the customs union between Russia, Belarus and Kazakhstan is developing rapidly. A number of agreements in the customs area have been signed by the customs union members. Some of these agreements (e.g. Customs Tariff of the Customs Union, Agreement on unified non-tariff regulation) are effective from 1 January 2010.
- Some other important documents (e.g. the new Customs Code and the customs valuation agreement) should come into effect on 1 July 2010.
- Recently Belarus representatives did not arrive to the meeting where the Agreement of the Customs Code of the Customs Union was signed by Russia and Kazakhstan. So the position of Belarus towards the customs union is under question.
- At the moment it is expected that starting from 1 July 2010 customs clearance of goods will be abolished between Russia and Kazakhstan.
- Further developments within the customs union (including amending of customs legislation) are expected during 2010-2011.

Customs Union: Potential benefits for business

- Dismantling of customs barriers within the customs union will give advantages for local manufacturers, companies operating consignment stocks, regional clusters, etc.
- On the territory of the customs union there will be unified customs regulations and customs tariff as well as unified non-tariff measures and technical standards (e.g. certification of conformity).
- Although VAT rates applicable in the member states of the customs union remain the same (12% in Kazakhstan, 18% in Russia and 20% in Belarus) indirect tax treatment in respect of goods, works and services transferred within the customs union is established (e.g. application of 0% VAT on sale of goods from Russia to Belarus and Kazakhstan).

Customs Union: Opportunities

- No customs tax liabilities in respect of conditionally released goods upon expiration of 5 year period. Goods which were customs cleared with exemption from customs duties are regarded as conditionally released (e.g. goods imported as in kind contributions to the charter capital). Importers are allowed to use conditionally released goods for designated purposes, only
- Companies having status of an authorized economic operator (AEO) may enjoy simplified customs clearance procedures (e.g. release of goods before submission of customs declaration, temporary storage of goods at AEO's premises). This is a cost saving opportunity for importers due to reduction of logistics and customs clearance costs. However, to obtain AEO status a number of requirements should be met (e.g. security of 1 mln Euros is required)

Customs Union: Opportunities

- Possibility to adjust customs declaration after goods release through customs may help in solving problems with overshipment/ misshipment of goods imported into Russia (special procedure for making such adjustments should be developed).

Customs Union: Risks

- Customs procedures for the Customs Union are still under development. This may lead to delays in customs clearance and disputes with the customs authorities
- The customs authorities have the right at their own discretion to suspend the release of imported goods which are subject to intellectual property rights (e.g. goods bearing trademarks) even though these trademarks are not included into the Customs Register by a trademark holder. As a result this may lead to delays in customs clearance and additional costs for importers. Based on the law, the importers suffered suspension of the customs clearance may claim from the trademarks holder to reimburse additional costs caused due to such suspension
- If the customs authority does not accept the customs value of imported goods they may suspend the release of goods until an importer makes the adjustment of the customs value. Currently, if an importer and the customs authorities do not reach an agreement about the customs value the goods could be released under a security for customs payments.

Customs Union: Risks

- Strengthened control of the customs authorities:
  - Customs control is extended from 1 to 3 years after goods' release by customs. Currently the statute of limitation for post customs clearance audit performed by the customs authorities is 1 year (although underpaid customs taxes may be collected for 3 years). .Starting from 1 July 2010 customs will have the right to perform post customs clearance control over imported goods within 3 year period. Thus, risk of assessment of additional customs taxes will increase
  - The customs authorities will be entitled to perform post customs clearance control in respect of any company possessing imported goods (currently, the customs authorities have the right to audit companies importing goods into Russia and wholesaling/ retailing companies)
  - Customs will be allowed to re-check the same goods during the next customs audit (currently, no repeat of the customs audit is allowed in respect of the same goods)

Thank you!

Natalia Vozianova
Partner, Tax services
natalia.vozianova@ru.pwc.com
Tel: + 7 (495) 967 62 37

Marina Volkova
Director, Customs services
marina.volkova@ru.pwc.com
Tel: + 7 (495) 967 62 23

Anton Shishkin
Manager, Customs services
anton.shishkin@ru.pwc.com
Tel: + 7 (495) 287 11 87

PRICEWATERHOUSECOOPERS

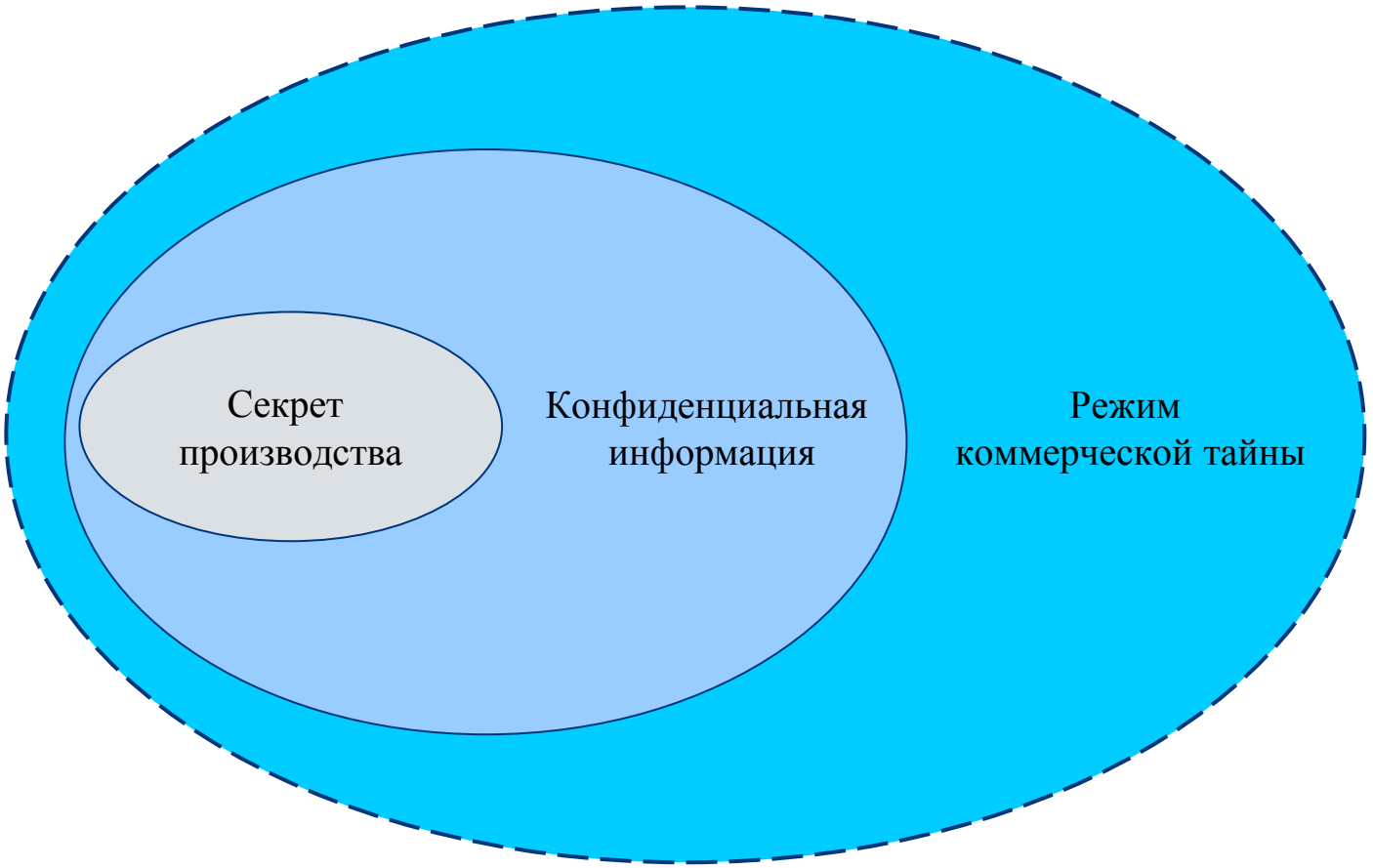
Актуальные аспекты защиты конфиденциальной информации

Круглый стол "Информационная безопасность и современные ИТ-решения для защиты информации"
03 июня 2010 года

Екатерина Карлова-Игнатьева

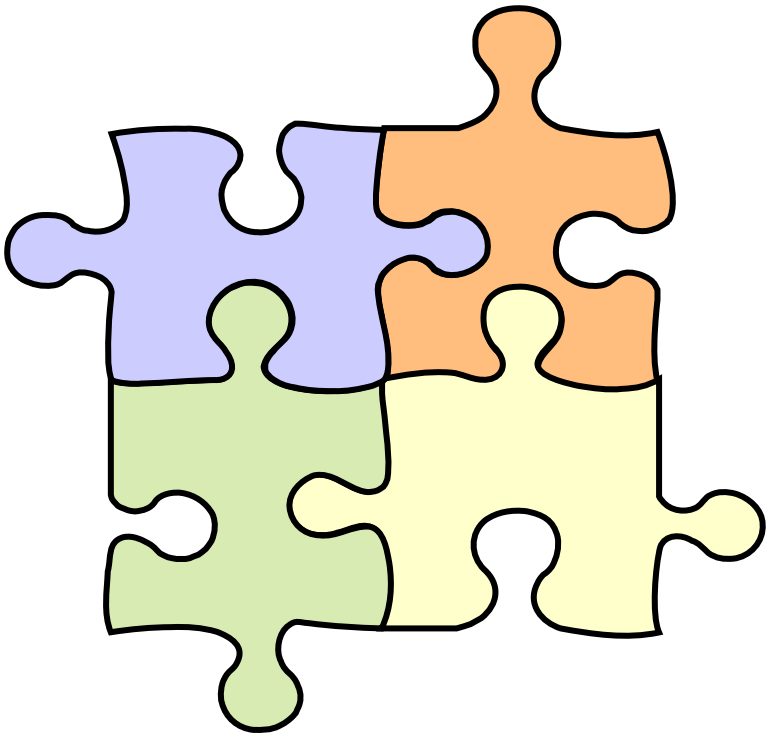
BEITEN BURKHARDT

Термины


Секрет производства
Конфиденциальная информация
Режим коммерческой тайны

Содержание

- Юридические аспекты
- Практические аспекты



Юридические аспекты

BEITEN BURKHARDT

Юридические аспекты

- Сведения любого характера, имеющие действительную или потенциальную ценность

- учредительные документы
- документы, дающие право осуществления предпринимательской деятельности
- о загрязнении окружающей среды, противопожарной безопасности
- о численности состава работников, о задолженности по выплате заработной платы
- о нарушениях законодательства*

* Указан неполный перечень

Условия предоставления защиты

Условия предоставления защиты

- Неизвестность третьим лицам
- Отсутствие свободного доступа к информации
- Введение режима коммерческой тайны

Режим коммерческой тайны

- Режим коммерческой тайны
  - Перечень информации, составляющей коммерческую тайну
  - Установление порядка обращения с конфиденциальной информацией
  - Учет лиц
  - Охрана в рамках трудовых отношений и при работе с контрагентами
  - Нанесение на материальные носители грифа “Коммерческая тайна”

Юридические аспекты

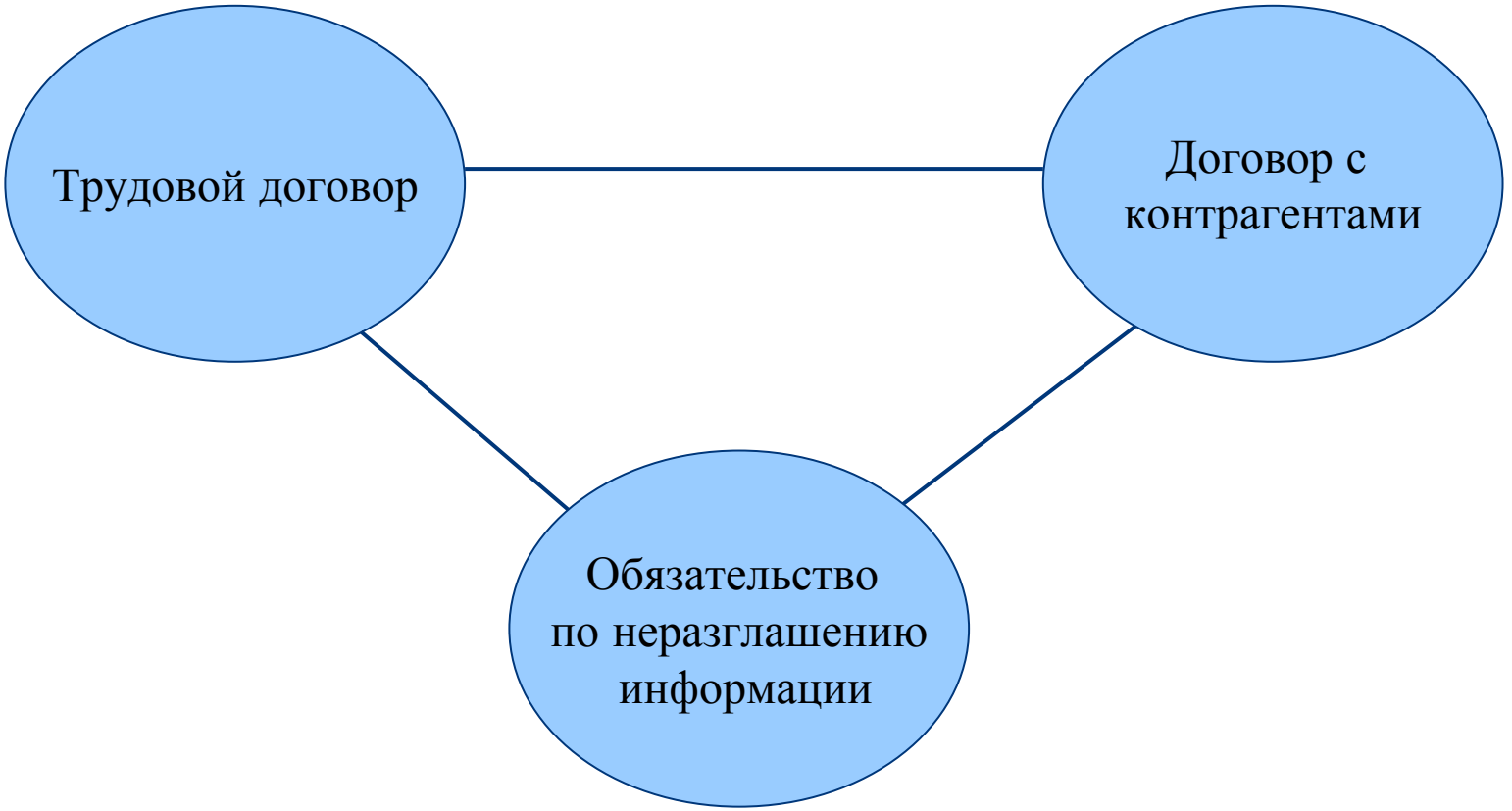
Положение о конфиденциальности

Перечень информации

Порядок обращения документов

Порядок учета лиц

Юридические аспекты



Практические аспекты

Практические аспекты

- Контроль
- Ограничение допущенных лиц
- Электронный документооборот
- Электронная почта

Контакт

- Екатерина Карлова-Игнатьева, LL.M
- БАЙТЕН БУРКХАРДТ
- Турчанинов пер., 6/2
- 119034 Москва

- Тел.: +7 495 2329635
- Факс: +7 495 2329633

- E-Mail: Ekaterina.Karlova@bblaw.com
- www.beitenburkhardt.com

Спасибо за внимание.

Cross Border Personal Data Transmission

Head Of Strategy, Corporate Affairs, & Legal Tele2 Russia

Mamuka Marhuliya

Points of Regulator's concern in Cross Border Data Transmission

- Central Data Warehouse at multinational companies Headquarters outside of Russia

- Ad hoc Data exchange between markets and HQ

- Cross Border Data transaction during global project execution: technical/IT projects, global marketing campaigns, etc.

- Access of expatriate employees to Billing units of a company or foreign contractors to Billing equipment

Regulatory Environment in Russian Federation

Law on Personal Data

- **Definition of Cross Border Personal Data Transmission (art.2):**

  Personal data transmission by an operator across the Russian border to a foreign state agency, a foreign individual or a legal entity

- **Restrictions on Cross Boarder Personal Data Transmission (art.12):**

  - Cross border data transmission is acceptable if a receiving country provides an *adequate* protection of personal data owners. *No definition of adequate protection is given*
  - Exhaustive list of exceptions are provided: Data owner's consent in writing, International Treaties, etc.

TELE2

Key Issues

- **Vague definitions in law:**
  - Loopholes in legislation and broad definitions let various authorities interpret law differently. *Example: Foreign personnel's access to Personal Data in Russia*

- **No definition of adequate Personal Data protection means:**
  - Russia Authorities do not apply principle of adequate enough protection of Personal Data in the countries ratified *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*
  - No official guidelines/recommendation to Cross Boarder Personal Data Transmission application available

- **No tracking mechanism of Personal Data Cross Border Transmission officially approved**

TELE2

Suggestions :

- More comprehensive definitions of Cross Border Data Transmission and its application are needed from authorities
- Authorities to consider best practice of international Personal Data processing
- Involve Personal Data operators in law making process

Thank You

Information Security and Modern IT-Solutions
for Information Protection

"Data Retention in EU Telecoms Regulation – The Case of Germany"

AEB IT-Telecom Committee

June 2010

Consulting
DETECON

Deutsche Telekom Group

Content

Preliminary Considerations

Rationale of Data Protection

Enhancing consumer confidence in the use of modern ICT and e-commerce services is of existential interest to operators and country's economic development.

Consumer Needs

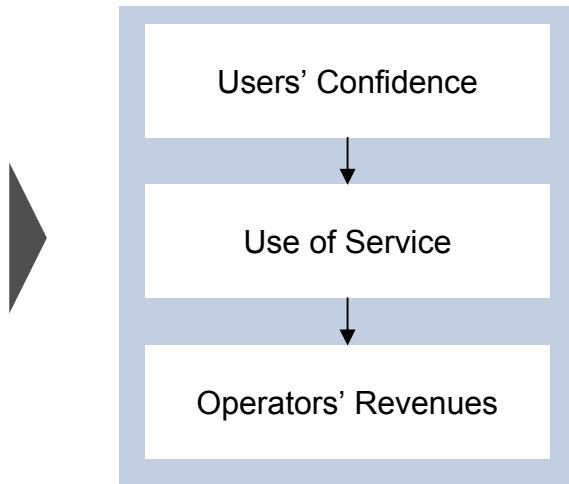
- Privacy of conversations
- Informational self determination

Business Needs

- Economic use of data
- Offering of new products/services
- Confidence of consumers in the use of services

State Needs

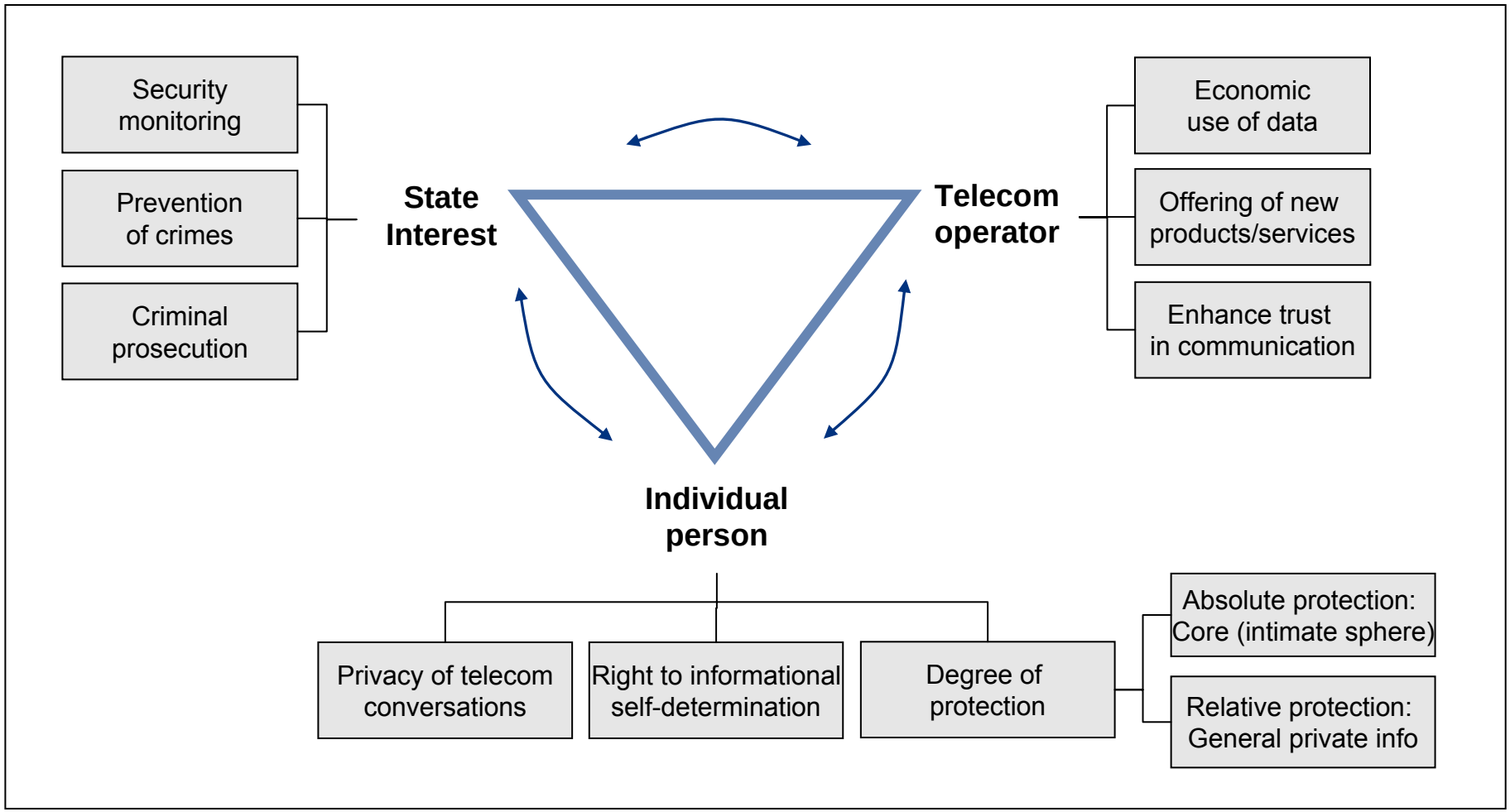
- Security monitoring
- Prevention of crimes
- Criminal prosecution



Preliminary Consideration

Main Challenge

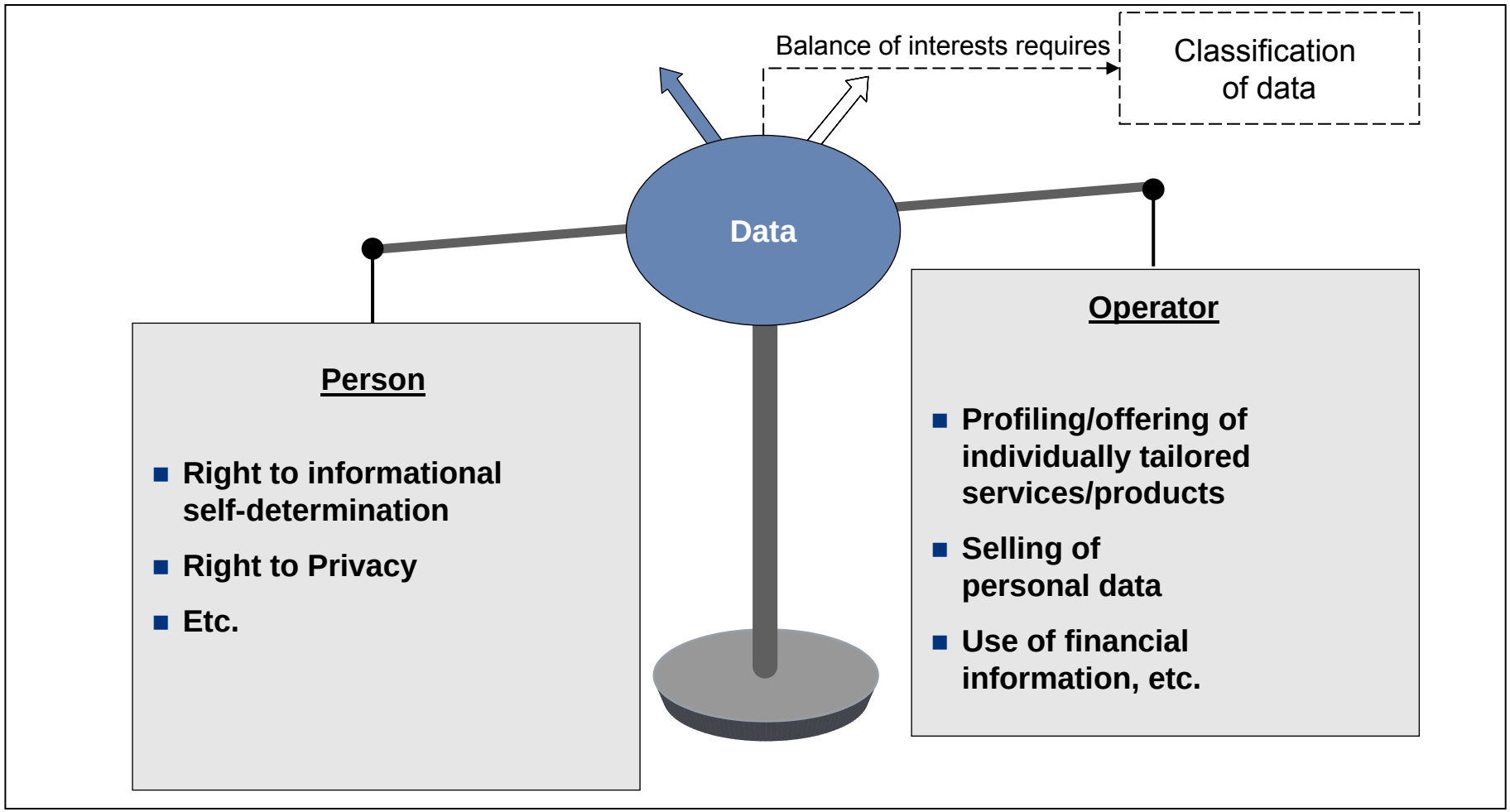
Addressing data protection requires adequate balance of interests of key stakeholders involved: State, telecoms operator and the individual person.



Preliminary Consideration

Operators' Interests vs. Individuals Interests

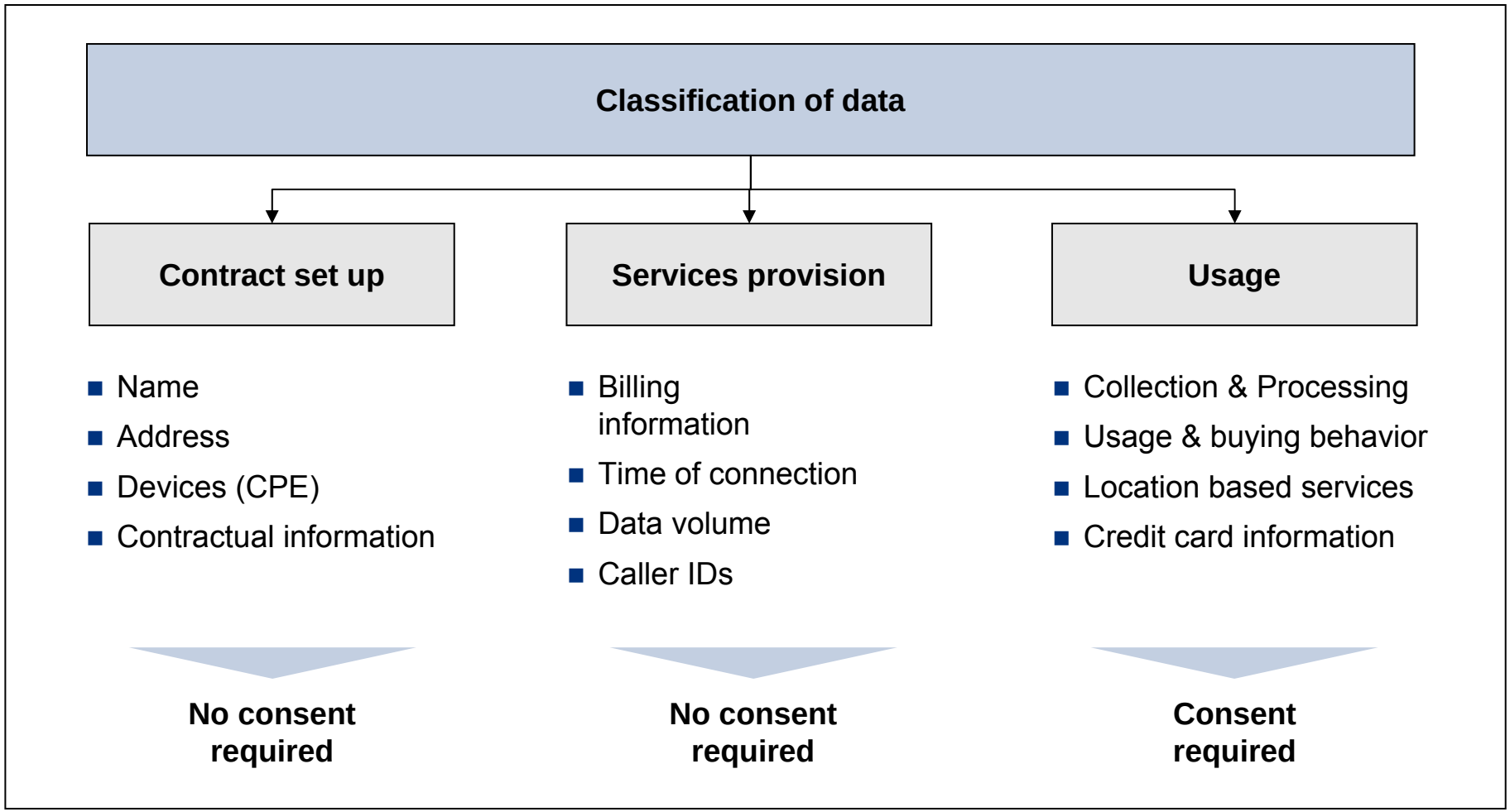
In order to balance the varying interests of the individual and the operator it is necessary to classify data and define what can be used with or without the individual's consent.



Preliminary Consideration

Classification of Data

Data are generally classified into three categories. Data categories decide on whether prior consent of the affected people is necessary for the use or not.



Content

Data Retention in EU Regulation

Scope of the Data Retention Obligation in Directive 2006

The data retention obligation in the Directive 2006/24/EC enables to know "who" has communicated or tried to do so "with whom" "for how long" and "from where".

Scope of the Data Retention Obligation in Directive 2006

To trace and identify…	Data Categories
The source of a communication	e.g. Calling telephone number; name and address of the user; Internet user ID
The destination of a communication	e.g. dialed number; number to which the call is routed; name, address & user ID of the subscriber & recipient
Date, time and duration of a communication	e.g. Date/time of the start/end of the communication; date/time of log-in/log-off of the Internet access service
The type of communication	The telephone service used; the Internet service used
User's communication equipment	e.g. calling and called phone numbers; IMSI/IMEI* of the calling/called party; DSL of the originator
The location of mobile communication equipment	Cell ID at start of communication; geographic location of cells by reference to their Cell ID

*IMSI: International Mobile Subscriber Identity; IMEI: International Mobile Equipment Identity

Data Retention in EU Regulation

Unsuccessful Action of Ireland

On 10th February 2009, the ECJ dismissed an action brought by Ireland to annul the Data Retention Directive on the ground that its legal basis was not appropriate.

28th April 2004	2005-2006	2006-2009
Proposal	**Position EU Commission**	**2006 action against the Directive**
■ France ■ Ireland ■ Sweden ■ UK	■ Art. 95 TEC Treaties is legal basis ■ Proposal to Council ■ 21st September 2005	■ Ireland with support of Slovakia ■ Request of annulment of the Directive by ECJ ■ Legal basis is rather in TEU, not TEC
Problem	**Adoption by Council**	**ECJ Decision 2009**
■ Legal Basis of a possible decision ■ TEC Treaties or TEU?	■ Directive 2006/24/EC on data retention ■ 21st February 2006 ■ Dissenting vote by Ireland and Slovakia	■ Art 95 TEC is appropriate legal basis ■ Arguments of Ireland rejected ■ Dismissal of Ireland's action

Content

The Case of Germany

Transposition of Directive 2006/24/EC in the Telecoms Law

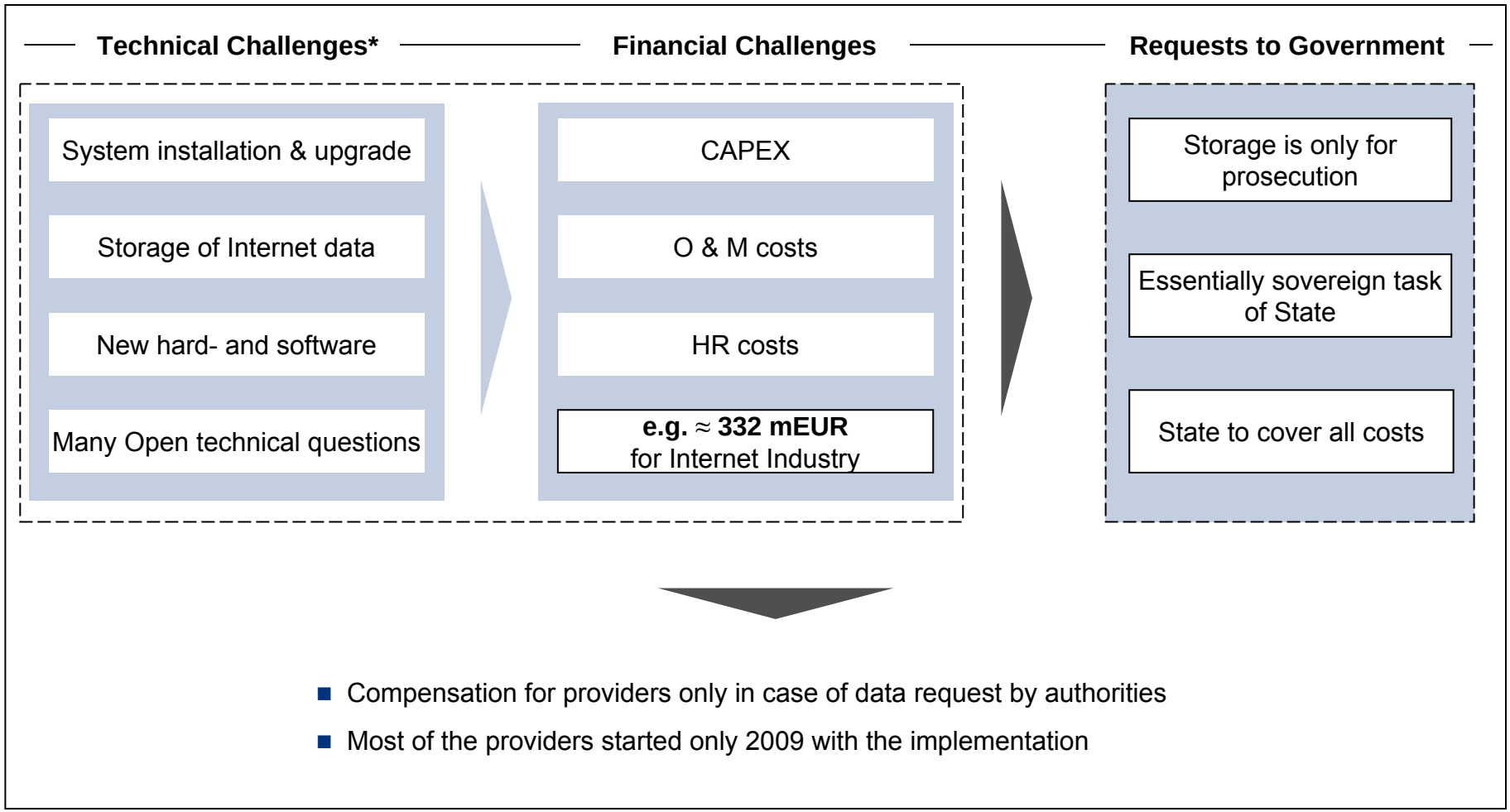
German telecoms law imposes a mandatory data retention period of 6 months and requires deletion at the latest 1 month after expiry. Content is not concerned.

Phone Services Providers	Email Services Providers	Internet Access Providers
1. Calling/called phone number, number to which the call is routed 2. Date/time of the start/end of the communication 3. Telephone service used 4. Mobile telephony • IMSI of the calling/called party • IMEI of the calling/called party • Caller/called Cell ID at start of communication • Date/time and Cell ID of initial activation of pre-paid service 5. Internet Telephony • IP address of caller & called party	1. Outgoing email • User ID of originator and recipient, IP address of originator 2. Incoming email • User ID of originator and recipient IP address of originating telecom equipment 3. Email retrieval • ID of email account and Internet-protocol address of retrieving party 4. Time of services use: Date and time	1. Allocated IP address 2. Precise ID of the account, from which Internet is used 3. Start/end and date/time of Internet use for the allocated IP address

The Case of Germany

Implementation Challenges for the Industry

The data retention obligations have substantial economic implications, as their implementation causes high investment and operating costs for service providers.



- Compensation for providers only in case of data request by authorities
- Most of the providers started only 2009 with the implementation

*BnetzA published only in December 2009 some technical guidelines

The Case of Germany

Judgment of Federal Constitutional Court (BverfGe)

According to the latest judgment of German federal constitutional Court, the current way data retention is structured in Germany is not compatible with privacy rights of users.

Complaints with BverfGe

- Storage of all telecoms connections without cause is disproportionate ("blanket")
- Facilitate creation of personality profiles and tracking of people's movements
- High costs of storage

- Privacy of telecoms communications
- Right to informational self-determination
- Freedom of occupation

Analysis of BverfGe

- Obligation as such to save data is not unconstitutional per se
- Possible creation of personality profiles and tracking of people's movements
- High risks of abuses

- No guarantee for data security
- No guarantee for Adequate restriction of the purposes of data use
- Transparency and legal protection requirements not met

Decision of BverfGe

- 2nd March 2010
- Current structure is not compliant with principle of proportionality
- National regulation for data retention not compatible with Art. 10 GG (Basic Law)

- The provision is as a whole unconstitutional and void

Operators have to delete all stored data "without delay". No transfer to authorities.

The Case of Germany

Data Security Requirements from BverfGe

According to BVerfGe, the existing framework does not meet the necessary data security standards resulting from the importance of data security in the context of data retention.

Constitutional Requirements

Data retention and data security

- Great importance of data security, given the scope and potential informative value of all gathered data

Legislative needs

- Legislation to provide a particularly high degree of security
- Essential provisions to be well-defined and legally binding
- Power to transpose the prescribed security standard into more concrete regulations may be transferred to a regulatory agency
- However, legislation to fix nature and degree of the relevant protective measures
- Decision should not ultimately lie without supervision in the hands of the respective telecoms providers

Existing Solution in the TA

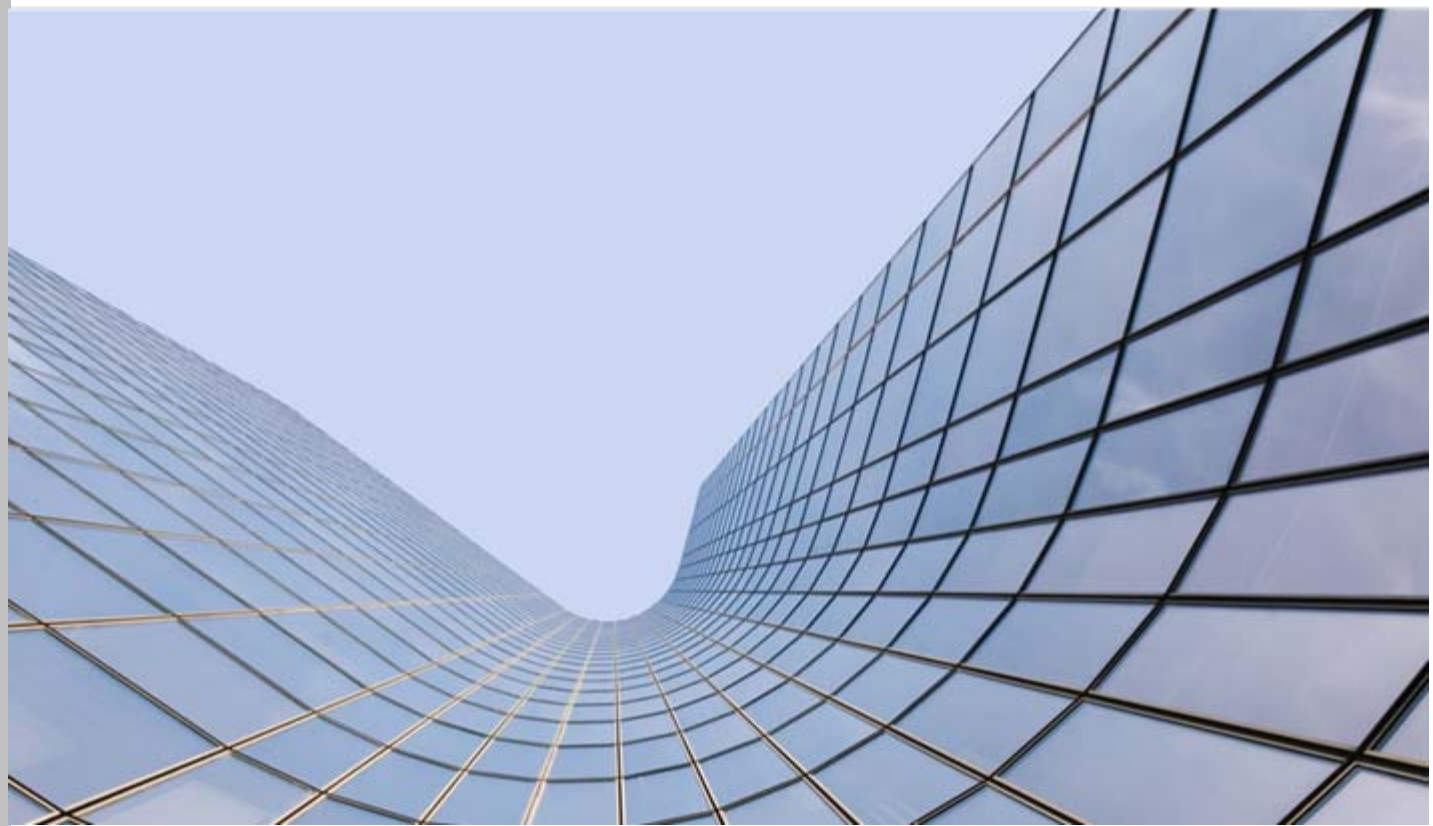
Data security standard

- The Telecoms Acts (TA) lacks the necessary guarantee of a particularly high standard of data security
- Reference essentially only to the care generally needed in the field of telecoms
- Security requirements remain undefined
- Security standards is left to the individual providers

Chief lacks in the TA

- No enforceable obligation for providers to ensure concrete security instruments, e.g.
  1. Separate storage
  2. Asymmetric encryption
  3. Four-eyes principle + authentication for access to the keys
  4. Audit-proof recording of access and deletion
- No otherwise guaranteed comparable level of security
- No balanced sanction system with at least same weight for data security violations as for storage duty violation

For more information contact



We Make ICT Strategies Work

Dr. Albert Njoume Ekango
Detecon International GmbH

Oberkasseler Str. 2
53227 Bonn (Germany)
Phone: +49 228 700 1536
Fax: +49 228 700 1507
Albert.Njoume@detecon.com

Jürg Zehnder

Regional Director Russia & CIS
Detecon International GmbH
Kotelnicheskaya nab. 29
115172 Moscow (Russia)

Phone +7 495 661 7834
Mobile +7 903 624 3243
Mobile +49 160 709 0209
Juerg.Zehnder@detecon.com