

No Transfer, No Trade

– the Importance of Cross-Border Data Transfers for Companies Based in Sweden



The National Board of Trade is a Swedish government agency responsible for issues relating to foreign trade, the EU Internal Market and to trade policy. Our mission is to promote open and free trade with transparent rules. The basis for this task, given to us by the Government, is that a smoothly functioning international trade and a further liberalised trade policy are in the interest of Sweden. To this end we strive for an efficient Internal Market, a liberalised common trade policy in the EU and an open and strong multilateral trading system, especially within the World Trade Organization (WTO).

As the expert agency in trade and trade policy, the Board provides the Government with analyses and background material, related to ongoing international trade negotiations as well as more structural or long-term analyses of trade related issues. As part of our mission, we also publish material intended to increase

awareness of the role of international trade in a well functioning economy and for economic development. Publications issued by the National Board of Trade only reflects the views of the Board.

The National Board of Trade also provides service to companies, for instance through our SOLVIT Centre which assists companies as well as people encountering trade barriers on the Internal Market. The Board also hosts The Swedish Trade Procedures Council, SWEPRO.

In addition, as an expert agency in trade policy issues, the National Board of Trade provides assistance to developing countries, through trade-related development cooperation. The Board also hosts Open Trade Gate Sweden, a one-stop information centre assisting exporters from developing countries with information on rules and requirements in Sweden and the EU.

www.kommers.se

Foreword

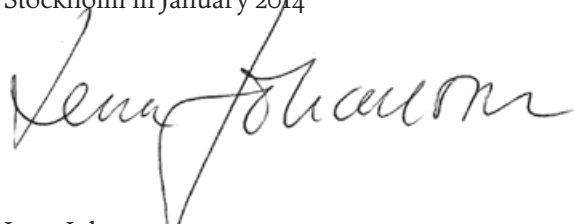
Today, business and trade is totally dependent on data flows – data that has to be moved in order to make trade happen and for efficient running of companies.

The world has gone digital and we live in an online society where digital solutions are a part of our everyday life. Internet and digital services affect companies, business models, consumer behaviour, what is traded and by who with whom. The possibility for companies, organisations, governments and individuals to move and share data is a precondition for this. While creating enormous opportunities, the digital age also raises important concerns, including the protection of personal information.

With this report, we hope to improve the understanding of the issue of data transfers, especially how companies use data transfers as part of their everyday trade and thus how data protection and regulations affect their business opportunities.

The report is written by Magnus Rentzhog and Henrik Jonströmer with the help of Emilie Anér and Robert Leijon. We wish to give our special thanks to company representatives for their time and willingness to discuss data issues with us.

Stockholm in January 2014

A handwritten signature in black ink, appearing to read 'Lena Johansson', written over a thin horizontal line.

Lena Johansson
Director General
National Board of Trade

Summary

The Internet has transformed international trade. The ability to move data across borders has been a vital part of this development and is now an intrinsic part of businesses' daily operations. Practically no company would be able to do business, or take part in international trade, without the ability to transfer data across borders. Data transfer is not confined to high-tech companies in the IT and communication sectors. Rather data is essential in all economic sectors.

In this study, the National Board of Trade shows how 15 companies in different sectors depend on data transfers either as part of their business offers or as part of processes within the companies. The interviews show that trade is inconceivable without data being transferred in some part of the transaction and all business models are based on data transfers.

Companies rely on digital solutions to sell and deliver their products. Data transfers between seller and buyer are necessary to initiate and complete a transaction as well as part of a continuous relationship. Moreover, many firms use third-party digital services, like cloud solutions, as part of the service offered to the customers and which depend upon the ability to send and receive data to and forth (for example) the cloud provider. Other firms are themselves suppliers of such services and depend upon data transmissions to ensure that other companies can supply their own services.

All the companies in this study also use data transfers as part of the internal running of the company. Data transfers are seen as necessary to ensure internal efficiency and that the business set-up is as effective as possible and suits the needs of the individual company. This includes moving human resources (HR) data to and from head-quarters, sending data to R&D facilities set up abroad or using cloud-solutions, and hence data transfers, to improve efficiency (by e.g. making information instantly available all over the world).

The use of the Internet and information and communication technologies (ICT), by individuals and firms generates huge amounts of data, including data relating to personal information. As the amount of personal data generated grows, so do concerns from individuals about how their personal data is being used. This is one reason why governments need to restrict the free flow of information across borders. Such restriction can take the form of legal requirements to store data within a country's borders and regulations that restrict the ability to move and process personal data across borders.

Based on the experiences of the companies interviewed, it is evident that data protection regulation that is too restrictive creates trade barriers and affects business models. Local data storage is the form of regulation that companies considered the most intrusive. Interviewees also underlined how the variances in different jurisdictions within and outside the EU lead to adaption costs and even missed trade opportunities.

A central problem for companies is how data regulation, especially restrictions on moving data to third countries, could entail missed business opportunities by increasing costs and inducing delays, making companies' prices unattractive or making products late to market. This also affects innovation. Another crucial issue is the administrative costs of ensuring compliance with data regulation.

Finally, companies transfer a lot of data to and back from the U.S.A. and U.S. companies. While this is usually unproblematic, various concerns were raised, including about using American subcontractors and about guarantees for protection of transferred data. Furthermore, using U.S.-based cloud solutions can be problematic due to fears of U.S. government access to the information and fear of data-leakage if stored data is transferred to third parties.

Sammanfattning på svenska

Internet har omvandlat internationell handel. Möjligheten att flytta data mellan länder har utgjort en grundläggande del av denna utveckling och är idag en central del av företagets vardag. I praktiken kan inte företag genomföra affärer, eller delta i handeln, utan möjligheten att föra data mellan länder. Dataöverföringar är inte bara en fråga för stora teknikföretag utan är väsentlig för alla ekonomiska sektorer.

I denna studie visar Kommerskollegium vilka behov av dataöverföringar 15 företag i olika sektorer har, antingen som en del av deras affärserbjudanden eller som en del av interna processer. Intervjuerna med företagen visar att handel är otänkbart utan att data överförs i någon del av transaktionen och alla affärsmodeller bygger på dataöverföring.

Företag använder digitala lösningar för att sälja och leverera sina produkter. Dataöverföringar mellan säljare och köpare är nödvändiga för att inleda och slutföra transaktioner och även som en del av ett långtgående affärsförhållande. Flera företag använder digitala tredjepartstjänster, som molntjänster, som en del av de tjänster de själva levererar till sina kunder. Här krävs att data sänds till och från molnleverantören. Andra företag är själva leverantörer av digitala tredjepartstjänster och använder dataöverföringar för att leverera sina egna tjänster.

Alla företag i studien använder även data som en del av interna processer. Dataöverföringar är avgörande för intern effektivitet, att företagen är organiserade så bra som möjligt och stöder företagets behov. Detta inkluderar att överföra personrelaterad data till och från högkvarter, sända data till utvecklingsenheter i andra länder eller använda molnlösningar (vilket medför dataöverföringar) för att öka effektiviteten (t.ex. genom att göra information tillgänglig i hela koncernen på en gång).

Användandet av Internet och IT-lösningar genererar stora mängder data, inklusive data som är kopplad till enskilda individer. Med en alltmer ökande mängd individdata så ökar farhågor kring hur data knuten till individer används. Detta är en anledning till varför regeringar behöver begränsa användandet av individdata och flödet av data mellan länder. Sådana begränsningar kan innebära bl.a. krav på lokal lagring av data och begränsningar i möjligheten att föra ut och bearbeta data utomlands.

Baserat på de intervjuade företagens erfarenheter så är det uppenbart att dataskyddslaggar som är för restriktiva skapar handelsbarriärer och påverkar affärsmodeller. Krav på lokal data-lagring anses, av företagen, vara mest hindrande. Intervjuade företag påpekade även att skillnaderna i hur data regleras i olika länder, inklusive inom EU, skapar anpassningskostnader och leder till missade affärsmöjligheter.

Ett centralt problem för företag är hur datareglering, speciellt överföringar till tredje land, kan leda till missade affärsmöjligheter genom ökade kostnader och förseningar, vilket kan leda till oattraktiva priser och försenade lanseringar. Det påverkar även innovation. En annan central fråga är de administrativa kostnader som efterlevnad av datareglerna medför.

Företag överför en hel del data till och från USA och till amerikanska bolag. Vanligtvis är detta problemfritt men intervjuade företag hade ändå en del farhågor, speciellt gällande användning av amerikanska underleverantörer och deras skydd av överförd data. Användande av amerikanska molnlösningar kan vara problematisk pga. oro för amerikanska regeringens tillgång till överförd data och rädsla för dataläckor om överförd data förflyttas till tredje part (vid t.ex. underhåll).

Index

Foreword	1
Summary	2
Sammanfattning på svenska	3
1. Introduction	5
1.1 Purpose and the plan of the paper	5
2. Defining data	6
2.1 Personal data and non-personal data	6
2.2 Different types of data used by companies	8
3. Why data must be moved cross-border	9
3.1 Using personal data.....	10
3.2 New and fast-growing business processes relying on cross-border data flows.....	10
4. Barriers to cross-border data flows	12
4.1 Two basic sets of barriers.....	12
4.2 Local storage and forced localisation	12
4.3 Personal data and data protection regulation.....	13
5. Data transfer needs and the experiences of companies based in Sweden	16
5.1 Companies' needs to transfer data to trade.....	16
5.2 The effect of data barriers on business models.....	17
6. Conclusion	23
Annex: 15 case studies	24
7.1 eBuilder – a cloud conscious about possible localisation requirements.....	24
7.2 Ericsson – global company facing restrictions in 180 countries	24
7.3 Google Sweden – “If you want to use the Internet, you must move data”	26
7.4 Hermes Medical – transferring data for medical and scientific purposes	26
7.5 HL Display – data transfers allow the bumble bee to fly.....	27
7.6 Klarna – regulatory patchwork hampers trade possibilities.....	28
7.7 NASDAQ OMX Stockholm – Safe Harbour simplify data transfers.....	29
7.8 Readsoft – using an American global supplier ensures security requirements for the cloud	29
7.9 Scania – using data in trucks has reached point of no return	30
7.10 Swedbank – bank services involving enormous data transfer needs.....	31
7.11 Tele2 – M2M-services cannot be developed and utilised optimally	32
7.12 TeliaSonera – looking for more restrictive Safe Harbour principles.....	33
7.13 TrustWeaver – compliance would equal unfeasible administrative burden.....	34
7.14 Volvo – data is a key asset that must be kept safe	35
7.15 [Manufacturing Company] – going global necessary despite reduction of flexibility.....	35
Literature	36
Notes	38

1. Introduction

Over recent decades, information and communication technologies (ICTs) and the Internet have grown to become a key enabler for productivity, innovation, and growth in the world economy. The Internet has accounted for 15–20% of GDP-growth in many countries, including developing countries.¹ The ability to move data across borders has been a vital part of this development. Thanks to the Internet and advances in technology, the volume of digitalised data has grown exponentially over the last decades. Today, researchers estimate that more data cross the Internet every second than were stored in the entire Internet just 20 years ago.²

Cross-border data flows are closely related to international trade. Nowadays, almost all firms in all economic sectors use electronic payment systems, Internet-based advertising and retailing, and cloud computing in their day-to-day operations. It is hard to imagine an international trade transaction that does not involve transferring data. Moreover, the growth of value chains, as well as the increasing dependency of services ('servicification') by manufacturing companies³, centres upon services and digital solutions and subsequently transfers of data.⁴ Transferring data cross-border has grown to become an important issue for trade as well as for the broader economy.

Personal data make up a large part of the data being produced and transferred. If one wishes to participate in modern society – by using digital solutions to communicate, browse, shop, share, and search information – it is impossible to do so without having personal data collected and spread across the Internet. This creates concerns about the protection of personal data and, as a consequence, governments place restrictions on data transmissions limitations that often affect companies' ability to trade. As such, restrictions on data transfers are automatically restrictions on trade. This is the main reason why the National Board of Trade has conducted this study. Being the governmental expert agency on trade and trade policy, the Board assesses the possible trade distorting effects of regulations.

This study does not intend to problematize the issue of protection of personal data. Personal data will only be discussed in relation to trade, especially the need to share data across borders, and

how regulations can affect trade in this context. The main purpose is to clarify how companies, in all sectors and of all sizes, use data in their businesses and the subsequent emergence of cross-border data flows in modern trade. However, since the Board has no expertise in the technical matter discussed, nor in aspects relating to data protection as such, the study relies on external sources for these discussions. Our interest is how international trade is affected.

By describing how companies use data, this study illustrates how complex trade is becoming. The trading world covers more and more topics and it is evident that trade rules must follow suit to support current business models.

1.1 Purpose and the plan of the paper

The purpose of this study is to show how companies use data transfers in their business models and for trade. The study will also explain how data restriction regulation can impact their operations and trade opportunities. This is done with the help of 15 case-studies of companies based in Sweden (presented in detail in the annex). The companies come from various economic sectors and include both large multinationals and small- and medium sized enterprises (SME) but do not represent a cross-section of companies affected by data regulation.

The study is structured as follows. In chapter 2, data is defined. Chapter 3 gives an introduction to the issue of cross-border data flows, explains the importance of data for business and international trade, and discusses the issue of personal data. Chapter 4 focuses on barriers to cross-border data flows, including the regulation of personal data. Chapter 5 is a summary of the 15 case studies and shows the importance of cross-border data flows for these companies. Concluding remarks are found in chapter 6.

The case studies are presented in detail in the annex. These case studies explain how each company relies on data transfers in their day-to-day operations and how data transfer regulations affect them.

2. Defining data

More data is being collected, processed, and transferred than ever before, and a large part of this data is personal data. This growth of personal data, and the ease by which such data can be transferred, is the foundation of the ongoing discussion about the right to transfer data across borders. However, while not all data is personal and thus not sensitive in the same way as personal data, it might still be affected by regulation aimed at protecting private data. Hence, it is essential to clarify the concept “data” and analyse what kind of data is being used and transferred.

Facts

What is data?

In relation to the Internet and data transfers, data can be defined as information that is held on a computer, or is intended to be held on a computer. Hence data is also information recorded on paper if it is intended to be put on a computer.⁵

2.1 Personal data and non-personal data

First of all, personal data must be defined. Broadly, it can be defined as data relating to an identified or identifiable person or persons⁶ or ‘everything a person makes and does online and in the world’⁷. This can include:

- User generated content, including blogs, commentary, photos, videos, etc.;
- Activity or behavioural data, including what people search for and look at on the Internet, what people buy online, how much and how they pay, etc.;

- Social data, including contacts and friends on social networking sites;
- Locational data, including residential addresses, GPS and geo-location (e.g., from cellular mobile phones), IP addresses, etc.;
- Demographic data, including age, gender, race, income, sexual preferences, political affiliation, etc.; and
- Identifying data of an official nature, including name, financial information and account numbers, health information, national health or social security numbers, police records, etc.⁸

Figure 1 shows what personal data can be in an individual’s life.

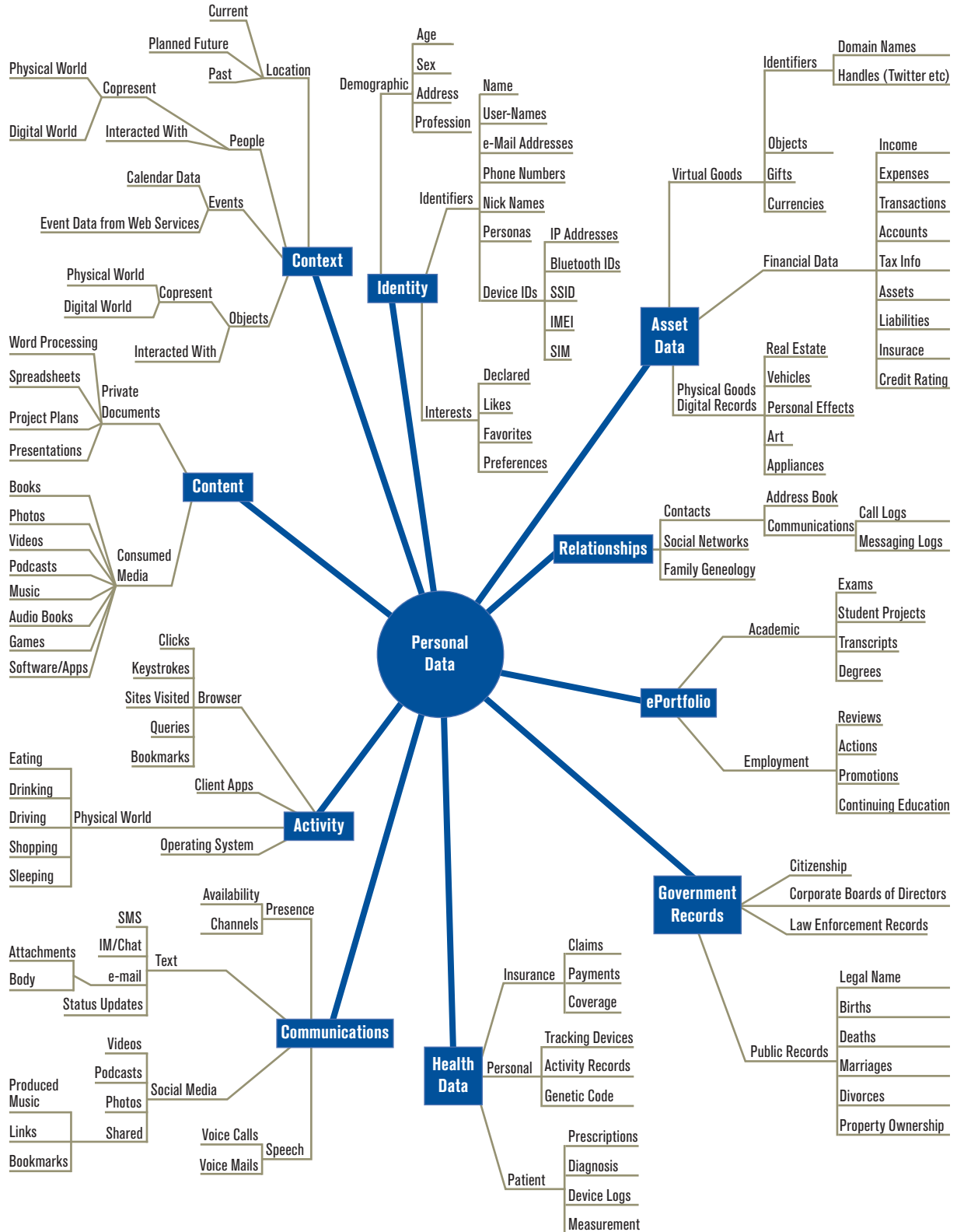
Data protection laws (more about that below) are set up to protect individuals’ personal information in all these data flows. Since the concept of personal data can be very broad, this can, as will be seen later, lead to uncertainties about what data protection regulations actually cover.⁹

Per this definition, all other forms of data are non-personal data. However, it is becoming more and more difficult to distinguish between personal and non-personal data. For example, modern techniques can often enable data relating to websites visited to be linked back to an identifiable person.¹⁰ This makes it hard to exactly identify what is personal data.

Personal data can be generated in the three different ways¹¹:



Figure 1: Summary of personal data in an individual's life



Source: WEF (2011)

- *Volunteered data* – created and explicitly shared by individuals, e.g., social network profiles.
- *Observed data* – captured by recording the actions of individuals, e.g., location data when using cell phones.
- *Inferred data* – data about individuals based on analyses of volunteered or observed information, e.g., credit scores.

Figure 2 describes how personal data can be generated (vertical axis). Each type of data is initially collected or accessed, then stored, aggregated, and processed, and then used/analysed (horizontal axis) – creating a data value chain. Each step can involve different stakeholders.

2.2 Different types of data used by companies

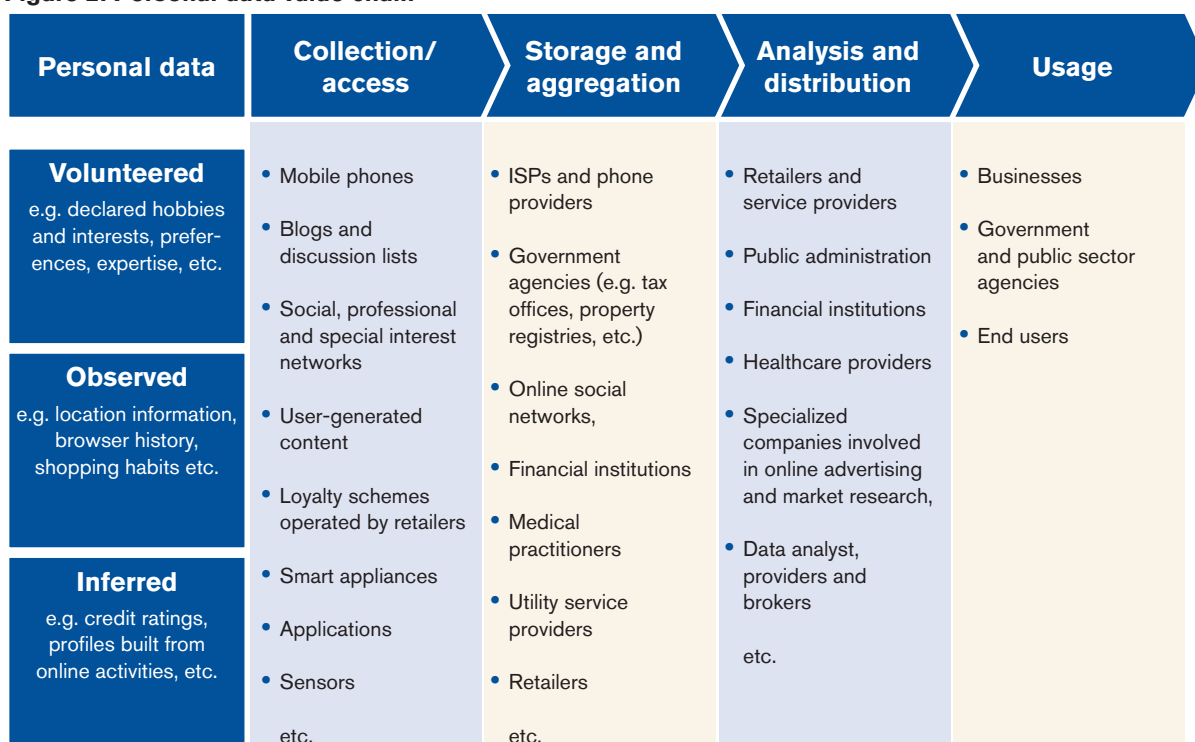
Beyond the notion of personal data, it is useful to distinguish between different types of data based on usage. When analysing what kind of data companies use in their operations, different types of data require being handled differently by firms. In table 1, the Board divides data used by companies

into five categories. All categories below might entail personal data. However, some categories involve more personal data than others and hence require different types of attention.

Table 1: Types of data used by companies

Types of data	Examples of data
Corporate data	Data about the company, including financial data, aggregated numbers about employees and web-site.
End-customer data (business-to-consumers, B2C)	Data about private people, including name, address, bank account, credit reports, phone number, and localisation of the phone
Human resources data (HR)	Data about employees, including names, e-mail addresses, salaries and competencies.
Merchant data (business-to-business, B2B)	Data about other companies, including name, address, contact person, customer registry, web-site and financial transaction data.
Technical data	Data about products, services and technical solutions, including the operation of these.

Figure 2: Personal data value chain



Source: OECD (2011) based on WEF (2011)

3. Why data must be moved cross-border

The Internet and ICT have in many ways transformed the global economy, including international trade. First of all, the Internet and ICT enable more services to be tradable. Roughly half of the global services trade is ICT-enabled, including cross-border data flow.¹² There is also a strong correlation between Internet usage and competitiveness.¹³ Secondly, the importance of geographical distance between producers and consumers has decreased considerably and businesses today can reach consumers in foreign markets in ways that were not previously possible.¹⁴ Thirdly, the Internet has contributed to the creation of completely new digital services that are easily tradable across borders. Computer software, e-books, mobile applications, and video and music streaming services are just a few examples of such services.

The use of the Internet and ICT is one reason why more data is being generated today than ever before – by individuals, firms, and machines. Data is generated in multiple ways: data can either be actively generated by individuals who provide it in traditional ways (by filling out forms, surveys, registrations, etc.) or generated as a by-product of other activities (for example, Web browsing, credit card purchases, and the use of mobile phones and tablets). Also, there is an increasing amount of data generated by machine-to-machine transactions.¹⁵

The growth of the Internet has also entailed the growing ability of people, businesses, and governments *to collect, share, and use data across borders*. The development of new technologies, products, and services in recent decades would never have been possible without the ability to freely move data across borders.

'Combining globalization with new technology and with new business models has dramatically accelerated the pace of change and innovation. The flow of data is as important as the movement of goods.'
USTR Froman (2013)

The use and transfer of data has grown to become an intrinsic part of businesses' daily operations. Practically no company, independent of sector, today would be able to do business, let alone take part in international trade, without the ability to transfer data across borders. For example, it is no longer possible to imagine a situation in which businesses were not able to use services and tech-

nologies such as e-mail, Internet browsing, or electronic payment systems.

In addition, it is more and more common for companies to centralise data for processing in one location. At the same time, the data must be instantly available globally for usage by company employees and agents.¹⁶ Data must be movable to one location and to all locations at the same time. Cross-border data flows are crucial for companies' day-to-day operations and moving data is about the ability to control and make operations more efficient.

It is important to underline that data transfer is not confined to high-tech companies in the IT and communication sectors. Rather data is essential in all economic sectors.¹⁷ It could be argued that data transfers are relatively more important for small companies than large.¹⁸ This is due to the fact that small companies have fewer resources to handle barriers and, additionally, using digital solutions like cloud computing can free relatively more resources for these companies.¹⁹ They are also more dependent on having the Internet as an efficient and cheap way to search for information.²⁰

Cross-border data flows have also been a driving force behind the emergence of so-called global value chains (GVCs) in which businesses' operations are fragmented across borders in order to increase efficiency, lower costs, and speed up production. Services are essential for the operation and efficiency of GVCs and are used to move the chain forward, to control the chain and individual tasks in the chain.²¹ With GVC being spread geographically, it naturally follows that data must be transferred for the chain to operate. Without moving data, today's GVCs cannot function. This is, of course, even truer for pure services value chains, which are built on digitalised services.²²

'Data needs to move to create value. Data sitting alone on a server is like money hidden under a mattress. It is safe and secure, but largely stagnant and underutilized.'
WEF (2012)

In sum, in order for companies to do business, be innovative, and stay competitive in global markets, they need to be able to send not only goods, capital, and competence (people) across borders, but also data.



3.1 Using personal data

The collection, use, and transfer of *personal data* have also grown rapidly. Every day, people send ten billion text messages, make one billion posts to a blog or social network and generate millions of entries into their electronic health records. With approximately six billion telephone subscriptions around the world, it is now possible to track the location, social connection and transaction of a very large number of people on the planet.²³ Using this information creates opportunities for firms, individuals, governments, and research institutions to create economic and societal value.²⁴ Personal data ‘is the new oil of the Internet and the new currency of the digital world’.²⁵

By collecting and analysing personal data, companies can better understand customers’ preferences and willingness to pay, and adapt their products and services accordingly. This ability to be responsive is an essential part of firms’ competitiveness today as well as their ability to trade. Oftentimes trade, especially trade to final consumers (B2C), cannot even take place without collecting and sending personal data across borders.²⁶ Additionally, personal data can also lead to new innovations based on a better understanding of customers.

3.2 New and fast-growing business processes relying on cross-border data flows

There are some business processes that exist solely due to the Internet and the ability to move data. Below, the Board describe, based solely on external

sources, three such new business techniques: cloud computing, big data, and the ‘Internet of Things’.

These techniques provide services and technologies that can help companies improve efficiency and reduce costs. The techniques are growing fast and expected to become increasingly important as businesses, individuals, and public entities become more reliant on the use of digital technologies.

Cloud Computing

Cloud computing is a way of providing IT functions such as data storage, processing power, and computer software as services over the Internet. This means that, as opposed to storing information and programmes on a personal or company computer, these things are stored on external servers that are accessed via the Internet. In this way, the cloud user can reduce the cost of both hardware and software.

Cloud computing is nothing new; e.g., web-based e-mail is a cloud computing service.²⁷ However, the scale is increasing immensely and more and more companies are looking at cloud solutions for cost savings and efficiency gains. This is especially true for SMEs and even individual consumers due to the explosive growth of so called smartphones (where a large majority of all applications are cloud based). The most-used cloud service is e-mail, followed by security, accounting/back office, databases, and online storage. Finance and manufacturing invest the most in cloud solutions.²⁸

Big Data

Another fast-growing area is so called ‘big data services’. The term refers to the *collection, storage, and processing of vast quantities of data*. As a result of the increasing digitisation of data and the decreasing cost of data processing and storage, new data management and analytics solutions – big data services – have evolved. These are able to process and analyse large and complex datasets that are difficult to process using traditional database tools and data processing application. The sector comprises suppliers of hardware and processing capacities for storage and analysis; data application developers; and entities (both public and private) that use big data services to produce other products and services.

Big data has the potential to help organisations, both public and private, improve efficiency, increase revenues, and reduce spending across a number of sectors. For example, it can help finan-

Example

How big data can be utilised

Using data to predict prices

Prices on the Web changes constantly, based on countless intricate factors. In 2012, a company called 'Decide.com' analysed four million products using over 25 billion price observations. With the help of algorithms, the company can foresee price shifts and advise customers on when to buy and when to wait. This helps customers buying online. One example of how Decide.com can help is to advise when to buy an older product as a newer version is being introduced. While most customers probably figure that the old version would now be cheaper, they might actually be more expensive, depending on when the customer clicks 'buy'.

Source: Mayer-Schönberger and Cukier (2013)

cial institutions use data on their customers in order to detect fraud or better determine customers' creditworthiness. Likewise, it can help manufacturers and retailers quickly adapt their production and services to changing consumer preferences. European public sectors can be made more efficient, reducing costs by 250 billion Euros per year.²⁹

Internet-of-Things applications and services

Today, it is not only computers and mobile phones that are connected to the Internet. Shoes, TVs, printers, cars, engines, and home appliance equipment, such as fridges and coffee machines, are just a few examples of devices that can be connected to the Internet today. These devices use embedded software that communicates with other devices and are commonly referred to as Internet-of-Things (IoT) devices. IoT applications and services can be used by governments, companies, and individuals to raise revenues, increase productivity, and reduce costs.³⁰

The Internet of Things also consists of industrial devices like machines or engines and are being utilised by manufacturing companies. IoT applications can be used to monitor the machinery used in

Facts

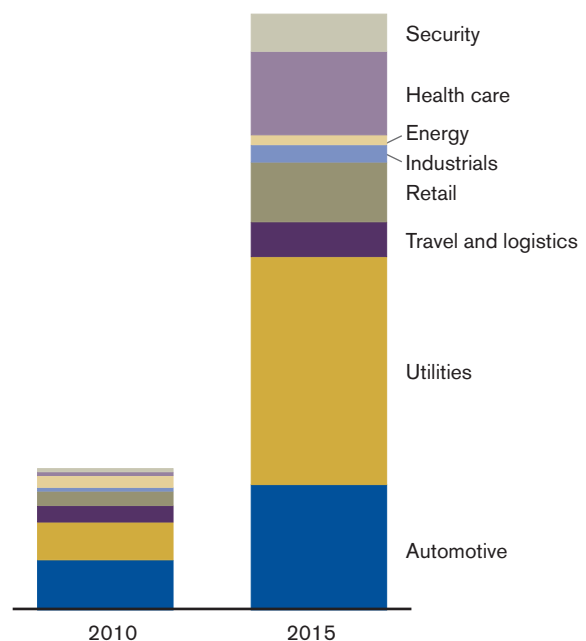
Internet of Things and trucks

Swedish trucking manufacturers, Volvo and Scania, equip their trucks so that they can transmit real-time vehicle location and diagnostic information to a central monitoring site. The system can alert drivers to when they need repairs and software upgrades, and can locate vehicles during emergencies.

manufacturers' own production (so-called process control) or to monitor the performance of products that have already been sold. For example, a single cross-country flight of a Boeing 737 generates 240 terabytes of data, much of which is used by the manufacturer to monitor and analyse the performance of the air carrier.³¹

The numbers of these IoT devices are expected to grow and reach 50 billion by the year 2020.³² A study by McKinsey projects that the number of IoT devices will grow at a rate over 30 per cent annually between 2010 and 2015.³³ As shown in figure 3, IoT is growing in many sectors of the economy.

Figure 3: Predicted growth of data generated by Internet-connected devices by sector (2010-2015)



Source: McKinsey Global Institute (2011)

4. Barriers to cross-border data flows

4.1 Two basic sets of barriers

Even though cross-border data flows are important for individuals, firms, and other organisations, governments need to restrict the free flow of information across borders in different ways. Such restrictions most commonly take the form of legal requirements to store data and locate data centres within a country's borders and regulations that restrict the ability to move and process personal data across borders.

In general, these two categories of barriers seem to be the most common and serious reported by companies, based on both previous studies³⁴ and interviews conducted for this study (presented in Chapter 5). It is important to note that other barriers to cross-border data flows also exist, such as Internet censorship and intellectual property regulation. These are however not discussed further in this study.³⁵

4.2 Local storage and forced localisation

Legal requirements on companies to either store data locally or only use local data servers have been identified by many as a serious and common impediment for companies that rely on the ability to move and process data across borders.³⁶ It has been argued that these types of restrictions are among the most potentially distorting trade measures currently being applied.³⁷

Local data storage requirements are usually motivated by concerns about personal data and are intended to prevent data from being misused. The argument is that if data is stored locally, the data will be more secure and governments will be in a better position to prosecute in case data privacy is violated.³⁸ The goal of forced localisation is usually to create investment or production of the establishments of foreign enterprises. Protecting personal information is usually not the main reason for this kind of regulations — they sometimes even have a protectionist foundation.³⁹ A large number of countries, both developed and developing, are imposing or planning to impose such requirements (see Table 2).

Forced localisation requirements mandate that foreign enterprises establish a data centre within a country as a condition for being permitted to provide certain digital services in that country. As an

Table 2: Countries imposing, or considering imposing, localisation or local data storage requirements

Types of ICT LBT	Selected Countries
Local IT infrastructure (such as data center) requirements	Brazil, China, Indonesia, Kazakhstan, Malaysia, Nigeria, Russia, South Korea, Ukraine, Venezuela and Vietnam
Local data storage requirements	Argentina, Australia, Brazil, Brunei, Canada, China, EU, France, Greece, India, Indonesia, Kazakhstan, Malaysia, New Zealand, South Korea, Taiwan, Turkey, Venezuela and Vietnam

Source: Own adaption of Ezell, Atkinson and Wein (2013). Norway and Denmark has been removed from their list since they seem to be based on a misperception. France should be treated with caution since it is limited to inception of data. However, the EU has been added under local storage.

example, Vietnam is planning to impose a law that would require companies' web search portals, data centres, and cloud computing services to be stored within the country. Likewise, Indonesia has a draft law that would require all data carriers, including mobile phone providers and foreign banks operating in the country, to establish local data servers in the country. Russia, Venezuela, and Nigeria have all passed laws that require IT infrastructure for payment processing to be located domestically.

Local data storage requirements imply certain restrictions on the processing and storage of data outside a country's borders. For example, Brunei, Greece, China, India, and Malaysia have laws that require that data generated within the country be stored on servers within the country. Two Canadian provinces, British Columbia and Nova Scotia, have implemented laws mandating that personal data in the custody of a public body (such as schools, universities, hospitals, and public agencies) must be stored and accessed only in Canada unless certain conditions are fulfilled. These laws, in turn, prevent such public bodies from using foreign digital service providers (such as cloud services) in cases where personal information could be accessed from or stored in a foreign country.

In the EU, Greece in 2011 adopted a law that forms part of the country's implementation of the EU's Data Retention Directive. The EU Directive requires Internet and telecommunication providers to retain certain data about a subscriber.⁴⁰ However, the Greek law goes further by requiring that retained data on 'traffic and localisation' stay 'within the premises of the Hellenic territory.'⁴¹ In light of the EU regulatory framework, it is unlikely that the



Greek requirement would still be in force but the Board has not found any recent information confirming or refuting that in the case of Greece.

In fact, as described in the National Board of Trade (2011), the types of regulation addressed in this chapter are contrary to EU legislation. Nevertheless, local storage requirements apply on the EU level. EU data protection regulation makes it clear that the basic premise is that personal data cannot be moved outside the EU.⁴²

Many countries also link local data storage requirements with forced localisation requirements. For example, India has proposed measures to require companies to locate part of their ICT infrastructure within the country.⁴³ This regulation would also require that the data of Indian citizens, government organisations, and firms not to be moved out of the country.

4.3 Personal data and data protection regulation

While forced localisation and local data storage are so far only restricted to a limited number of countries, regulations controlling personal data are commonplace. This type of regulation also affects companies more often in their day-to-day operations. Consequently, this study will describe these types of barriers in more detail.

The vast amount of personal data being collected, used, and transferred to other countries and to third parties brings with it concerns about personal data and control over one's own data. As the amount of personal data generated grows, so do concerns from individuals about how their personal data is being used.

As of 2013, 99 countries have adopted some form of data protection and privacy legislation that restricts the use and transfer of personal or other sensitive data.⁴⁴ This form of regulation is primarily intended to protect individuals' right to information privacy and to prevent the misuse of personal information. Companies across in all industries must comply with such laws and this can cause problems, either because laws are overly burdensome or restrictive, or because legal frameworks across countries differ, which in turn creates compliance costs and unpredictability for firms.

4.3.1 Data protection in the EU

The Data Protection Directive

The European Data Protection Directive⁴⁵ came into force in 1995 as a response to the lack of harmonised data protection laws across EU Member States.⁴⁶ Prior to the Directive, some Member States applied strict limitations and procedures, while others had no rules at all. This diversity was seen as a barrier to the movement of information in the EU and the development of the internal market. The twin objectives of the Directive are: (1) to protect the rights of individuals with respect to the processing of their personal data; and (2) to facilitate the free movement of personal data between Member States.

The Directive sets out a number of conditions under which personal data can be gathered. Furthermore, persons or organisations that collect and manage personal data must protect it from misuse and respect certain rights of the data owners, which are guaranteed by EU law. The Directive allows the transmission of personal data to third countries but under the condition that the country in question is

deemed to have an adequate level of protection. In essence, 'adequate' has been interpreted as equivalent⁴⁷ and to date, the European Commission has found only eleven economies⁴⁸ to have such adequate protection.⁴⁹ Nevertheless, the need to transfer data has been remedied in other ways, notably by the so-called Safe Harbour agreement with the U.S.A. (see chapter 4.3.3.).

The Directive has been implemented differently across the EU Member States and companies in the EU dealing with personal data still have to deal with 28 different data protection rules. This causes uncertainty, administrative burdens, and costs for companies dealing with personal data in the EU.⁵⁰

The proposed Data Protection Regulation

In response to new technological developments, an increased use of personal data, and the lack of harmonisation of data protection laws across the EU, the European Commission in 2012 made a proposal for a new legal framework in the form of the *General Data Protection Regulation*⁵¹. The Regulation is aimed at modernising EU data protection legislation, so as to meet the challenges resulting from globalisation and the use of new technologies, while at the same time strengthening individuals' rights to information protection. Once adopted, the Regulation would become a single law applicable across the EU, hence reducing the variety in data protection rules caused by the current Directive. At the time of writing, discussion about the specific content of the regulation is still on going. The adoption is aimed for 2014 and the Regulation is planned to take effect in 2016.

Under the proposed Regulation, companies would only have to turn to the Data Protection Authority (DPA) in their home-country for issues relating to data protection. An important feature of the proposed Regulation is that it, unlike the current Directive, would apply to organisations based outside the European Union if they process personal data of EU residents.⁵²

The proposed regulation includes a number of new requirements on firms in order to strengthen the protection of personal data in the EU. For example, it requires firms to develop data management systems that allow for greater flexibility such as data portability (the right of individuals to transfer data from one electronic processing system to another) and the right of individuals (data subjects) to obtain personal data in a commonly used electronic format. So-called 'data protection impact assessments' must also be incorporated into firms' IT project management so that they can identify and mitigate specific risks associated with the pro-

cessing of personal data. All firms (and public sector bodies) with 250 employees or more must also designate a 'data protection officer' (DPO) who will act as a firm's main point of contact with the DPA. In addition, both data controllers (entities that determine why and how personal data are to be processed) and data processors (entities that process data on behalf of the data controller) must ensure that the DPO is involved in all issues that relate to the protection of personal data and maintain detailed documentation on all processing operations.⁵³

As for transfers to third countries (that are not deemed as adequately protecting data), the idea is to give appropriate safeguards by, in particular standard data protection clauses, binding corporate rules and contractual clauses. The option of contractual clauses gives some new flexibility to companies, but is subject to prior authorisation by supervisory authorities.

Facts

The Right to be forgotten

The Right to be forgotten⁵⁴ is also worth mentioning (since several of the companies in the annex raised concerns about this obligation). This right to consumers poses an obligation on the company or organization to delete any personal data if there is no legitimate reason to keep it. This right would be granted to an individual even though consent has been given to store or handle said personal data. The right to be forgotten would thus entail a right for the individual to withdraw consent, even years after it has been given. There is some room for interpretation on how far a company would have to go in order to retrieve personal data once it has been repeated on the web elsewhere. If this provision was to be interpreted in a broad manner, it could entail some workload for companies keeping track of data they have been given consent to distribute, or even data that is distributed by the individual himself via a provider or platform. It is at this early stage difficult to appreciate the extent of the changes and work required by such proposal for companies. Several actors have however already warned that it would require substantial investments.⁵⁵

4.3.2 EU versus U.S. data protection regulation

As stated above, different countries approach the issue of data protection differently, sometimes creating difficulties for those wanting to transfer data. The two largest global traders, the EU and the U.S.A., have different approaches to data protection regulations.⁵⁶ This in turn creates problems for both EU and U.S. firms wishing to transfer and process personal data as part of their business models/offers. Considering the paramount importance of transatlantic trade for both the EU and the U.S.A., it is important to understand the different approaches to the regulation of personal data.

The EU has a so-called 'omnibus approach' to the protection of personal data with region-wide data protection regulations. In contrast, the United States has a sectoral approach to personal data, with specific provisions tied to particular sectors and/or forms of data.⁵⁷ For example, there is one law regulating the collection, disclosure, and sharing of financial information, and another on health-related information. The US also has a law that regulates online collection on and use of personally identifiable information on children. In addition, federal authorities such as the Federal Trade Commission and the Department of Health and Human Services, together with various authorities on the state level, have the right to adopt and enforce privacy regulations.

Another difference between the EU and the U.S. approach to personal information is that while the EU obliges data processors and controllers to ensure that data subjects enjoy the benefits of data protection even if personal data is processed outside the Union, U.S. data regulation do not offer similar protections.⁵⁸

4.3.3. Ways to mitigate differences between regulatory approaches

Generally, EU regulations are considered to be the strictest of all such regulations of personal data in the world. Moving data out of the EU is, as a point of departure, forbidden. A central exception from this rule is that data can be transferred to countries with 'adequate' protection. However, this has been interpreted to mean 'equivalent' (hence, the limited number of countries regarded as safe destinations). Currently, however, the U.S.A. is not considered as having an 'adequate' level of protection. For companies located in the U.S.A. and other countries not deemed having 'adequate level of data protection', there are still some options for being allowed to process personal data linked to EU citizens.

Companies in the U.S.A. have the option of signing the *Safe Harbour Framework*. This has been developed by the US Department of Commerce, in collaboration with the European Commission, and is a voluntary and enforceable code of data protection practices. By adhering to the framework, US companies declare their compliance with EU data protection standards and are allowed to process data on EU citizens. Compliance with the agreement is indirectly enforced as members of the agreements have to certify their adherence to the programme by annual declaration to the Department of Commerce and by publicising a privacy policy statement.⁵⁹ It is important to note that the Safe Harbour framework is only open to entities that are subject to the jurisdiction of the Federal Trade Commission (FTC) and thus excludes important sectors such as banking and insurance, as well as many intra-company traders and back office functions.⁶⁰

Binding Corporate Rules (BCRs), another option under EU legislation (open to not only the U.S.A.), were developed to allow multinational companies, international organisations, and groups of companies to make intra-organisational transfers of personal data across borders in compliance with EU data protection rules. BCRs typically form a rigorous, intra-corporate global personal data policy (for example, rules with the company group) that satisfies EU standards and may be available as an alternative means of authorising transfers of personal data outside of Europe. BCRs are required to be approved by the data protection authority in each EU Member State in which the organisation will rely on the BCRs.⁶¹

Model Contract Clauses (MCC) can also be used. A 'model contract' is a general type of contract that includes specific provisions dealing with data protection, and that has been approved either by the EU Commission or by the Data Protection Commissioner. A data controller in the EU who wishes to transfer personal data to third countries can use the model contract as the basis for its relationship with the third-country organisation. There are two different types of model contract: (i) a contract to facilitate the transfer of personal data between a data controller in the EU and a data controller outside the EU; and (ii) a contract to facilitate the transfer of personal data between a data controller in the EU and an agent or subcontractor (data processor) located outside the EU.

5. Data transfer needs and the experiences of companies based in Sweden

In this chapter, interviews with 15 companies based in Sweden are summarized.⁶² This summary will show how they all rely on data transfers. The chapter goes on to discuss how data protection regulations affect their businesses. In the annex, the interviews are presented as detailed case studies. The Board refers the reader to the annex for a full range of examples, requirements, and concerns when it comes to moving data across borders and how data protection affects their business models.

The companies chosen in this study are from different economic sectors and are of different sizes. The Board tried to map a large variety of companies to underline that data transfers are essential for all kinds of companies. However, the companies are not representative for all companies that might be affected by data protection regulation.

5.1 Companies' needs to transfer data to trade

Data transfers are closely linked to trade and necessary for making trade happen and companies depend on moving data as part of their interna-

Table 3: Examples of why different types of data need to be transferred to make trade happen and run businesses

Types of data	Examples why data transfers are needed
Corporate data	To coordinate between different parts of a company To sell goods and services
End-customer data (B2C)	To sell goods and services For developing new products For enabling outsourcing To provide support 24/7
Human resources data (HR)	To coordinate between different parts of a company To match skills
Merchant data (B2B)	To sell goods and services For developing new products To provide support 24/7
Technical data	To sell goods and services To up-grade software To monitor the running of a product For developing new products For enabling outsourcing To provide support 24/7

The examples are taken from the interviews found in the annex.

tional operations. The needs of the 15 interviewed companies can be divided into two categories; as part of their business offers and as part of processes within the company or company group. The former can be described as improving external efficiency while the latter is about internal efficiency.

Table 3 illustrates different reasons why the companies in this study need to transfer data for running their operations.

5.1.1 Data transfer as part of a business offer

All interviewed companies rely on digital solutions to sell and deliver their products (goods or services). They use data transfers in three ways.

First and foremost, this includes the actual services delivery (for example, online services), but also includes sending data about customers, be they private individuals (B2C) or other companies (B2B) – billing, marketing, online payments, and so forth. Hence data transfers between seller and buyer are necessary to initiate and complete a transaction.

Following from this, companies also use data transfers in their ongoing relationships with their customers, such as delivering software upgrades, monitoring the running of products (Internet of Things), or analysing efficiency and detecting repair needs. This can also be the result of consumer demands for support (or access to the service) around the clock. As such, data transfer needs between buyer and seller are continuous and not a one-off transaction.

Secondly, several of the firms in this study use third party digital services, such as cloud solutions, as part of the services offered to the customers (i.e., they use these services). In these cases, the companies are dependent upon the ability to send and receive data to and from (for example) the cloud provider. If this is not possible, the firms cannot deliver their services to their customers.

‘The significance of data in any ICT solution is irrefutable, like the blood stream in a human body; one cannot exist without the other.’
Summer (2013)

Thirdly, some of the companies interviewed provide digital infrastructure services (e.g., telephone services) or function as the supplier of a third party digital service (e.g., a cloud supplier), that is, they offer these services. These companies function as



facilitators for others and depend upon data transmissions to ensure that other companies can supply their own services. In these cases, a restriction on the ability to transfer data will in turn affect other companies' abilities to deliver their services.

Another central point is that the companies have put a lot of effort into making online solutions and data transfers as efficient as possible. Finding and using the right 3rd party service provider is also a central issue for companies. Data is used to build global value chains and to fragment production, allowing companies to specialise in certain tasks. Here data transfers are used to ensure the efficient running of operations, a lowering of costs, and – in the end – the ability to stay competitive. Likewise, the ability to centralise data *processing* in one location, usually in Sweden in the case of our interviews, is a fundamental reason for the companies to move data. Data processing becomes more efficient and, as a result of this, so does the business offer.

The data transferred in all these instances includes both end-customer and merchant data; however, a large portion is also technical data. This involves both personal and non-personal data.

5.1.2 Data transfers for internal processes

All the companies in this study also use data transfers as part of the internal running of the company. Data transfers are seen as necessary to promote internal efficiency and to ensure that the business set-up is as effective as possible and suits the needs of the individual company.

Most companies interviewed need to move human resources (HR) data to and from headquarters.

Another reason for moving data is to send it to R&D facilities set up abroad. Hence, data must be moved to allow for product development. In addition, without the ability to move data, the cost of setting up R&D units abroad would be higher and some companies would not be able to tap into the skills that, in many cases, are not found in Sweden.⁶³

Several of the companies use cloud solutions, and hence data transfers, to improve efficiency. One reason put forth by a number of the interviewees was that cloud solutions allow for instant information access for all employees at any time, in any location. This is considered important for transparency, efficient work methods, and, in the end, competitiveness.

Data transfers are also necessary for outsourcing processes. The outsourcing partner must have access to relevant data in order for the outsourcing solution to be effective.

Data that needs to be transferred to ensure increased internal efficiency are identified in table 3. This also includes both personal and non-personal data.

5.2 The effect of data barriers on business models

While the above section primarily deals with reasons for companies to move data, this part concentrates on how data protection regulation can affect business models and trading opportunities. This section is mainly based on the views expressed by the companies in the interviews.⁶⁴

The case studies underscore that data protection regulations have implications on most sectors of the economy. Data protection regulations affect all sectors and cannot be labelled as just an ICT-only issue. This is a central point as the debate tends to focus only on the effects on large cloud providers⁶⁵ or high-tech companies. Almost all companies use the Internet and if someone (or something) is linked to the Internet that means data can be shared across borders.

'It is a fundamental mistake to think of the digital economy as just Google, Amazon and Facebook when also traditional European manufacturing and services – in short, everything from car production and shops to logistics – all depend on data and connectivity.'
Lee-Makiyama (2013a)

In fact, data regulation also affects SMEs and low- and middle tech companies. Together the low and middle tech companies account for 80 per cent of GDP⁶⁶ in Europe and are the largest users of digital solutions. Efficiency gains for this large body of companies might be affected by data transfer restrictions.⁶⁷

5.2.1 Data protection regulation's positive impact on business models

All company representatives interviewed support data protection. Some even want to see more protection of individual's data.⁶⁸ However, since this study is about how regulation can become restrictive, the reader might get the notion that companies consider data protection regulation as something that is simply a burden. This is not the case.

Although, interviews focused on barriers, some companies gave examples of how data protection regulations have a positive impact on their businesses.

Furthermore, one company noted that restrictions on how to handle personal information has led them to scrutinise what data they collect and why (this concerned especially internal processes). In this way, personal data was protected while internal processes were streamlined.

Finally, some companies raised the fact that the demand for data to be stored in the EU can be a selling point. Their customers tended to feel safer knowing that the data was stored in the European Union, i.e., in the same jurisdiction. This builds trust.

5.2.2 Data protection regulations affect trade in all sectors

All companies interviewed confirmed the title of this study: no data transfers, no trade. Trade is inconceivable without data being transferred in some part of the transaction⁶⁹ and all the business models are based on data transfers.

A number of examples were put forward about how data regulation that is too restrictive has affected trade. A central problem was how data regulation could entail missed business opportunities by increasing costs and inducing delays, making companies' prices unattractive or making products late to the market.⁷⁰

Barriers to cross-border data flows also reduce the ability to adopt the most efficient technologies and services as part of their business operations. The best examples of this are barriers that prevent the use of cloud computing services, which are used to outsource both software and hardware and therefore increase efficiency and reduce costs. The most serious impediment to the use of cloud computing is localisation requirements, which effectively makes the use of cloud computing impossible. Regulations relating to personal data can also act as a barrier to the use of cloud computing since transfers to entities outside the EU are restricted. Some companies highlighted the fact that these restrictions on data movement lead to a situation where processing has to be done in several locations instead of preferably in one central (usually non-European) location.

Data protection regulations also influence investment decisions.⁷¹ One company described how restrictions that were too onerous in one EU member state hindered them from entering a market.⁷² This is a clear example of direct effects on trade—missed business opportunities.

Some companies offering services to consumers stressed the fact that barriers to moving personal data became an obstacle since it makes it harder for companies to identify customers.⁷³

In the interviews, companies put a lot of emphasis on restrictions on moving data to third countries. For them, this is a central obstacle. As noted in chapter 4.3, the European Commission has found only 11 economies to have adequate enough data protection to allow for the free movement of data from Europe. However, these economies only cover 6 per cent of the global services trade (see

Table 4: Share of world trade in services and ‘adequate’ protection of personal data

World top 15 Servicetraders (80% of world trade)	Share of world services trade	‘Adequate’ privacy legislation
EU27	23,5%	
United States	15,1%	No
China	6,9%	No
Japan	4,9%	No
India	4,7%	No
Singapore	3,8%	No
Korea, Republic of	3,2%	No
China, Hong Kong SAR	3,1%	No
Canada	2,9%	Yes
Switzerland	2,4%	Yes
Russian Federation	2,2%	No
Australia	2,0%	No
Brazil	1,7%	No
Norway	1,6%	EEA country
Thailand	1,5%	No

Source: ECIPE (2013). Note that data transfers are services while non-services companies are also affected by data protection regulations.

table 4). Data can only be freely transferred to a very limited group of trading partners.

EU data protection regulations are relatively strict policies compared with other countries. This implies a competitive disadvantage for EU firms vis-à-vis competitors in other countries (mainly the U.S.). While the discussion above is based on companies’ experiences with current EU legislation, it is worth emphasising that proposed EU data regulations in some areas will impose even stricter requirements on European firms. This will, according to one study,⁷⁴ in turn reinforce the negative effect on European firms’ international competitiveness.

Focusing on trade flows between the EU and the U.S.A., and assuming current solutions for data transfers (see chapter 4.3.3.) are no longer recognized,⁷⁵ one study⁷⁶ estimates the effect of the proposed regulations on firms could have a -0.8 to -1.3 per cent effect on EU GDP. Exports from EU could drop by 6.7 per cent due to decreased competitiveness. Due to the importance of services for manufacturing, goods exports could also decline by 11 per cent. SMEs would be affected the most.

5.2.3 The burden of compliance

All regulation entails compliance issues; data protection legislation is no different. However, the

questions are rather ‘what kind of compliance?’ and ‘how does it affect business?’

There are two main types of compliance costs: administrative (e.g., new routines and processes) and operational (e.g., local storage).⁷⁷ Focusing here on administrative costs, all companies declared that they work hard to ensure compliance with data regulation. One company noted that their main problem with data protection regulation is the time and administration needed to review and implement different legal variations, both within and outside the EU. Some companies have solved the problem of differences in standards between countries by adopting internal rules based on the highest standards found.

Complying also includes negotiating contracts to ensure data safety and to clarify data ownership. Likewise, ensuring compliance when outsourcing or using cloud services takes a lot of time and money. Many times, companies need to buy external guidance to get compliance right, especially when building or rolling out new systems or services. Some firms see compliance costs as negligible while others highlighted the costs they incur. Building data systems in which individuals tick boxes to indicate acceptance of handling of personal information is also costly.⁷⁸ For example, one company has three lawyers working full-time to ensure compliance.⁷⁹ One study estimates that the cost to the U.S. national economy for just reading privacy policies is 365 billion USD.⁸⁰

According to the European Commission (2012b), the overall administrative burden of the directive on data protection is 5.3 billion Euros (2.9 billion is due to fragmentation within the EU). Another study estimates that the overall compliance costs borne by a single large company average 2.5 million Euros per year. A large part of these compliance costs are due to the fragmentation of national data protection rules (both within and outside the EU).⁸¹ A study by the UK Ministry of Justice concludes that the proposed data protection regulation will have, for the UK alone, an extra annual net cost of between £100 million and £360 million a year.⁸²

In addition, compliance costs can be a rather significant issue for smaller companies. One study states that compliance for non-ITC SMEs can add up to a 40 per cent increase on IT budgets.⁸³ Pomonon (2011) and Commission (2012b) confirm that small companies incur substantially higher costs than larger ones.

Facts

SMEs and compliance costs

A study by Christensen et al. (2013) estimates the administrative costs created by the proposed regulation for EU SMEs in particular, concluding that the average SME can expect its annual cost to increase by between approximately 3,000 and 7,200 Euros, depending on the industry in which the SME is located. This in turn represents 16 and 40 per cent of current annual SME IT budgets. These estimates take into account the positive economic effects for SMEs (e.g. reduced costs for firms caused by only having to deal with one common EU Data Protection Agency⁸⁴).

5.2.4 Data protection affecting innovation

Clearly, data protection is costly and a lot of the discussion about the proposed EU legislation has, as seen, focused on compliance costs. Moreover and perhaps more importantly, regulation affects innovation.

Many companies interviewed have R&D units, or work with third party suppliers, outside the EU. This means that not all data can be shared with those needing to develop new services or processes. Sometimes, companies cannot use cloud solutions to connect different R&D units since this would automatically entail data transferring. Lack of consent from data owners also contributes to the inability to use available data.

The 'shielding' of information, the result of not being able to send data, usually means delays in product development and higher costs. Some companies also described how they have to use second-best partners for their development needs.

An interesting effect is how this situation has led companies to change modes of delivery—not being able to move data to developers means moving the developers to the data. That is, in this case, replacing cross border data flows with the movement of natural persons, which in turn implies other obstacles (e.g., the cost of moving developers and their families, immigration procedures, and costs).

A specific concern raised was innovation in sectors with rapid product cycles, where gains from one product are used to finance the next. Here, delays due to data protection compliance (usually due to notification obligations⁸⁵) can be very dis-

ruptive. A missed opportunity due to data protection regulations compromises the ability to finance the next innovation.⁸⁶

Literature shows that data protection regulations affect innovation across all sectors of the economy, including manufacturing.⁸⁷ Also, the effects on innovation are more problematic for SMEs than large companies.⁸⁸ Finally, it must be noted that while the discussion on the effects of data protection tend to focus on the high-tech sectors, the effect is probably as big in low-tech industries.⁸⁹

The European Parliament (2012) examined the likely impact of the EU's proposed General Data Protection Regulation on innovation among European firms. They found that although the regulation offers many potential advantages, it tends to be overly prescriptive in areas where European firms have already demonstrated compliance and adherence to important concerns regarding the protection of personal data. The study concludes that the regulation risks impeding innovations among European firms.

5.2.5 Different barriers, different concerns

Companies have varying levels of acceptance concerning different types of regulation. Regulations aimed at protecting personal information, like for example demands for consent for data transfers, are generally seen as less intrusive. Although they can be costly and cumbersome to manage, companies accept them. That being said, several companies claimed they would welcome the removal of some demands for consent or clearer rules on when consent is needed.

In contrast, no company saw merits in regulations on forced localisation or local storage. These types of regulations are seen as very intrusive, costly, and could even force companies to leave territories (especially smaller markets where the extra costs cannot be born).⁹⁰ However, the companies interviewed had less of a problem with having to store it in the EU as compared to a single member state. While not optimal, EU storage was seen as less interfering.

Interviewees also highlighted the need to handle data differently depending on the type of data. As exemplified in tables 1 and 3, companies handle diverse forms of data with different degrees of sensitivity. More sensitive data require more safeguards and there are clear differences between personal information and technical product data. Neverthe-

less, as seen above, data protection does not always make this distinction, especially not localisation regulations.

5.2.6 Companies want harmonisation of rules

Data protection regulations need to be harmonised. This was a clear message that emerged from the interviews. The intra-EU patchwork of different legislation and legal interpretations ought to be removed. Some also want harmonisation with countries outside the EU—or at least fewer different rules.⁹¹

Interviewees underlined how the variances in different jurisdictions lead to adaption costs and even missed trade opportunities. As seen in chapter 5.2.3, the current fragmentation is costly. One of the companies described how the regulatory differences lead to delays in rolling out new services since they wish to do this in all markets at the same time. Another company concluded that differences lead to uncertainties and a hesitation to share information, even inside the company. Hence harmonisation and also clearer rules would be very beneficial to companies.⁹² “Data protection cannot mean data protectionism” as Neelie Kroes, Vice-President of the European Commission puts it.⁹³

On the difference between regulation in EU and non-EU countries, the interviewed companies are not necessarily looking for full harmonisation, i.e. bringing non-EU countries up to the EU-level. Rather the companies think that the optimal solution would be to have high standards of protection in other countries – high enough to be considered adequate to live up to EU standards without being as stringent as is the case today.⁹⁴

5.2.7 Technology and secure data transfers

Regulation is not the only way to safeguard personal information and to ensure safe data transfers. Technology and a well-developed communications infrastructure are also important tools for securing data.

Technology complements regulation when it comes to protecting data. Securing the integrity of data and avoiding leaks are essential when handling data, not least for data processors. A number of companies in this study emphasised the need to build secure systems to avoid breaking national data laws. This is also seen as a competitive advantage, especially when working with clients in countries where concerns about personal information are par-

ticularly high. The companies also emphasised the fact that an efficient way to secure data and make it less vulnerable is to spread it out geographically, that is, store data in different countries.⁹⁵ In fact, spreading data to different jurisdictions increases security and flexible access since users/owners of data are not at the mercy of a single country.

‘Data transfers are not the weak link but a necessity for secure data’

Mothander and Hernell (2013)

Robust security systems must be put in place to ensure safe data transfer and storage. This is, of course, a challenge as costs rise. Notably, many companies use different levels of security for their data needs. Personal data is transferred in systems with higher security than technical or corporate data. One company declared that working with a large global supplier increases the security of their clients. According to this company, these suppliers have more resources to build secure and compliant systems than smaller suppliers.

Additionally, security must be weighed against speed. Users must not experience delays in transfers, irrespective of their location in the world. As such, speed is essential for the interviewed companies and their clients, especially since business models oftentimes demand instant access to information and data sharing without geography making a difference. Hence, for data transfers to be effective and for data to be secure, technology – particularly communications infrastructure – is essential. The infrastructure must allow for instant transfers of huge amount of data as well as security measures.

5.2.8 EU-U.S. transfers – somewhat of a headache

For natural reasons, the U.S.A. was the non-EU country that most often came up in discussions. Most companies have a presence there, work with U.S. sub-contractors or use services offered by U.S.-based companies. Hence, the need to transfer data to and from the U.S.A. and U.S. companies is tremendous. Overall, business, including data transfer, works well. Nonetheless, several problems are evident – stemming from laws and actions on both sides of the Atlantic.

Some of the interviewed companies considered the way that data protection is handled in the U.S.A. could lead to problems as companies sometimes cannot use subcontractors based in the U.S.A.

Often it depends upon the fact that the U.S. partner cannot provide the guarantees needed to satisfy EU legislation. Curiously, a specific concern is actually that some of the largest U.S. companies work with standardised contracts that, according to these Swedish companies, do not give enough data protection.⁹⁶ The contracts mean that companies from the U.S.A. cannot provide enough guarantees for the protection of data in those instances.

Furthermore, many firms find the patchwork of U.S. legislation hard to understand and penetrate. The extra-territorial effect of some legislation is also problematic. This can be the ability to both fulfil the requirements of the legislation (see, for example, the companies in the financial services sector in the annex) and use the services offered by firms from the U.S.A. Many companies, using U.S.-based cloud solutions, witnessed how customers hesitate to use their services since data will be stored on servers belonging to companies from the U.S.A. This gives rise to two concerns: first the fear of the U.S. government being able to access the information stored on those servers, and, second, worries about data-leakage if stored data is transferred to third parties by the cloud providers. It is difficult to assess how much this, in the end, affects the companies⁹⁷ – but companies have to put extra effort into winning new customers or evaluating cloud solutions.

Some companies use the Safe Harbour Framework for their transfer needs. On the whole, it works well. Nevertheless, there are criticisms. One specifically concerns how Swedish companies must ensure that U.S. partners fulfil the demands, and that they must inspect the partners. One company said that the Safe Harbour standards should be higher since it is hard to negotiate with newer companies as they tend to have a too relaxed attitude towards data protection. A stricter Safe Harbour would force them to raise their standards.

5.2.9 Unforeseen consequences

During the interviews, companies provided several illustrations of how data protection regulations can lead to unforeseen consequences. One example is how restrictions on moving data can put a strain on research. Cloud services are commonly used in research projects to share and process scientific data, including medical data. Barriers to data transfers can incur difficulties for researchers and could delay medical advances and treatment of patients.

Some companies explained how data protection affects the internal running of companies. A typical case in point was the movement of data on personnel – even for purely internal reasons – hindering skills-matching and working with equitable salary levels within a company group.

Another example was how personal data can be used to instantly detect fraud, for example, when it comes to financial transactions. Data protection regulation does not allow companies to handle criminal information. Regulation can at the same time hinder the setting up of processes that aim to deter and report non-ethical and criminal actions. One company describe how their whistleblower programme⁹⁸ can be hard to implement since it involved acceptance by local data inspection agencies and the consent from those that could be reported under the system.

5.2.10 Knowledge of data protection regulation

It is evident that knowledge of data protection regulation varies considerably among companies based in Sweden. The companies in this study were all aware of applicable rules, but their views on how to interpret them differed. Moreover, interviewees gave a number of examples of how many Swedish companies lack awareness of data protection regulations and an understanding of how those rules might affect their businesses. It was argued that many companies are affected by data protection regulations but are not aware of this. This might have repercussions on the safety of individuals' personal data—especially since this seems to be an EU-wide situation.⁹⁹ This lack of awareness and understanding of the rules might have a trade impact as investors hesitate to invest due to uncertainties.¹⁰⁰

Interviewees often came back to the fact that regulation is not adapted to the business realities of today and how companies need to move data to ensure efficiency and competitiveness. Here it is worth repeating that the companies are not against data protection rules as such. Far from it: all the interviewees expressed support for protection of personal data. However, it was deemed important for regulators to understand how data protection can negatively impact businesses and competitiveness. There are concerns that excessively high standards of protection in Europe (and Europe already has the highest standards) will impact companies' competitiveness. For the companies, a balance between protection and the ability to move data was important.

6. Conclusion

This study underscores that trade cannot happen without data being moved from one location to another. The Internet and ICT solutions enable many services to be traded and have created new services. This is trade in digital form, that is, by sending data. Furthermore, people, companies, and machines using the Internet create enormous amounts of data. The use and transfer of this data is a fundamental part of businesses' daily operations. Practically no company, independent of sector, can do business, let alone take part in international trade, without the ability to transfer data across borders.

At the same time, some data, notably personal information, must be handled with care. The underlying question for regulators is how to strike the right balance between these two (the need to transfer data and the protection of personal data), at times contradictory, concerns.

The study does not aim address the question of balance. The aim of the Board is to explain how companies use data transfers in their business models and to trade. This study also explains how data restriction regulations can impact operations and trade opportunities. Based on the material presented, the Board would like to highlight the following key messages that interviewed companies put forth.

First and foremost, data is about all companies and not just large tech-savvy companies. As much as anyone else, SMEs in low-tech sectors depend on data and data transfers to operate and stay competitive. As such, regulating data protection must imply assessing the needs and concerns of a wide variety of companies.

Secondly, regulation should focus on certain forms of data, not all of it. Data localisation regulation in particular tends to encompass all types of data, including purely technical data. To minimise trade effects, regulation should be as focused as possible.

Thirdly, of the two types of regulation primarily discussed in this study, companies are more concerned with the adverse effects of forced localisation and similar regulation. This type of regulation is much more intrusive and should, according to the companies, be done away with. Regulation concerning the protection of private data is also important to address but here companies question the present balance between protection and transfers.¹⁰¹

Fourthly, harmonisation is important for companies and companies would like to see differences between EU members removed. In addition, removing some differences between regulations in the EU and other countries (especially the U.S.A.) would facilitate business. In fact, the larger the area where data can freely be transferred, the lower the transaction costs for companies.

Fifthly, companies look for clearer and more predictable rules. One problem today is that there are a lot of grey areas (for example, what is personal data?) and companies tend to interpret the rules differently.

Finally, companies hoped that the ongoing negotiations between the U.S.A. and the EU (TTIP – Transatlantic Trade and Investment Partnership negotiations) can be an opportunity to discuss data transfer and to remove some obstacles. Companies feel that governments on both sides of the Atlantic can work both individually and together to ensure and facilitate trade. Here it is also important to note the modal complementarity that is raised under 5.2.4 and the fact that if data protection restricts data movement, governments must ensure movement of natural persons in order to not jeopardise R&D and innovation.

The Board concludes that this study illustrates how complex trade is becoming. The trading world covers more and more topics and it is evident that trade rules must follow suit to keep up with current business models.

Trade rules used to be about goods crossing borders. Then negotiations recognised the importance of services trade (both on its own and to support manufacturing trade). Today, manufacturing is becoming more and more dependent upon services and the Board argues that negotiators must start handling goods and services together in order to support trade. Governments should discuss 'goods AND services', not 'goods or services'.¹⁰² In addition, as shown in National Board of Trade (2013d), the movement of natural persons is ever more becoming a prerequisite for making trade happen. Hence, negotiators must handle the movement of people too. Now, to fully keep up with business, negotiations must look at movement of data. Cross-border movement of data is the new oil in the machinery of trade. Hence, negotiations that support actual trade must now be about goods AND services AND people... AND data.

Annex: 15 case studies

For this study, the Board interviewed 15 companies based in Sweden about how these companies use data transfers in their businesses. The Board also wanted to understand how data protection regulations, from the companies' point of view, affect their operations. The result is presented in this chapter and gives the reader an in-depth understanding of how data is used and how regulation might make business more complicated. The case studies are based on the companies' own stories and how they themselves view data protection issues.¹⁰³

7.1 eBuilder – a cloud supplier conscious about possible localisation requirements

eBuilder is a Swedish supplier of 'Cloud Processes for Value Networks',¹⁰⁴ or commonly called BPaaS,¹⁰⁵ with more than 100 companies and governmental authorities as customers. Every year, eBuilder handles hundreds of millions of business transactions, between more than 70 countries worldwide, for some very big company brand names. The company is headquartered in Stockholm with an R&D office in Sri Lanka and local sales offices in China and Australia. The hosting of eBuilder global Cloud Services is done in Sweden (that is, servers are in Sweden), but the company has support and consultant services in all local offices.

eBuilder needs to move data through physical borders, among countries for at least three reasons. The first and major reason is related to the business eBuilder is doing for its customers. It is the need for data to flow between Sweden, where the cloud hosting is done, and the worldwide countries that are involved in all eBuilder's cloud processes,¹⁰⁶ operated on behalf of their customers. This covers markets where eBuilder customers request them to integrate eBuilder's global subcontractors,¹⁰⁷ to be able to operate the end-to-end business processes. Second, as eBuilder is a global company, it also needs to move its own employees' personal data between Sweden and Sri Lanka, China, and Australia. Finally, also related to eBuilder's internal processes, the R&D staff in Sri Lanka and Australia need access to eBuilder's internal IT infrastructure and the sales staff need access to information relating to customer concerns. The two last aspects are

important from an eBuilder internal efficiency point of view, while the first is related to eBuilder's existence as a cloud service provider overall.

The main worry from eBuilder, when it comes to data transfers and storage, is the growing tendency of forced localisation/storage of data within physical borders/countries. eBuilder would instead welcome countries to more strongly emphasise how technical solutions can guarantee security aspects and drive global standards. Forced localisation/local storage entails potential costs as eBuilder must be able to guarantee local storage in several places worldwide, plus fulfilling multiple supports for multiple laws and regulations. Hence, contracts must perhaps be renegotiated and, at times, new subcontractors found. Another aspect is some different countries' 'supervision' of electronic communication, like the 'Great Firewall of China'¹⁰⁸ and thus the lag on performance of data when communication is done in and out of those countries. According to eBuilder, business transactions/data as 'orders, invoices, etc.' ought to be certified and handled outside 'threat supervision', that is the supervision by, for example, the FRA in Sweden and NSA in the U.S.A.

Beyond this, eBuilder (itself an outsourcing contractor) also relies on their customers to manage their own privacy and legal aspects of their data, which are communicated via Sweden, for eBuilder to run and support.

7.2 Ericsson – global company facing restrictions in 180 countries

Ericsson is a world-leading provider of mobile network equipment and software, as well as professional services for managing network and business operations. Ericsson's portfolio also includes products for broadcasters, cable operators, OTT Video, CDN, mobile payments, e-health care, and connected car solutions. The core business is network solutions (55 percent of net sales), followed by services (40 percent). Ericsson is the 5th largest global software company. Ericsson is present in over 180 countries and headquartered in Stockholm, Sweden. The company employs about 112,000 people, out of which 57,000 work in services—locally or from regional services centres. 24,000 work with R&D, an area of central interest to Ericsson.¹⁰⁹



Over 1,000 networks in more than 180 countries use Ericsson's network equipment. More than 40 percent of the world's mobile traffic passes through Ericsson networks, 1.4 billion mobile consumers are charged and billed through Ericsson's solutions, and Ericsson manages the operations of networks that serve more than 1 billion subscribers. With this in mind, it is virtually impossible to describe all the data transfer needs of Ericsson. It is, however, safe to say that data transfers are an indispensable part of Ericsson's business.

Being a global company in an extremely high-tech and fast evolving business, data protection regulations have large effects on the company. Ericsson is affected by data protection regulations in all jurisdictions they operate in. Some key issues regarding cross-border data flows that Ericsson faces include:

- Outright prohibitions of personal cross-border data flows to a foreign country.
- Outright prohibitions of employee cross-border data flows within Ericsson group to a foreign country.
- Extensive, lengthy, complex, slow, and unpredictable procedural burdens of national Data Protection Authority approvals of data transfer agreements.
- Forced localisation of IT/server infrastructure.

Some of the restrictions above are, according to Ericsson, international trade barriers as they bar the possibility of Ericsson (or any other foreign multinational company) consolidating operations across multiple territories. Ericsson cannot reap the

benefits of economies of scale that are necessary to offer competitively priced services to enter a national market.¹¹⁰ In a similar way, prohibitions on exporting employee data across borders within the Ericsson group has limited the opportunities for Ericsson to match the best skills available and compete more successfully.

Other barriers increase transaction costs associated with cross-border data transfers, which leads to missed business opportunities, delays in project execution, and unnecessary increases in unproductive administrative costs.

Finally, some restrictions do not prohibit or increase the cost of cross-border data flows as such, but rather take away the economic incentive to compete in a national market by forcing Ericsson to invest in local IT/server infrastructure. Here, Ericsson is free to move the data but will face local costs of excessive infrastructure resulting in disadvantageous cost structure, ultimately making the business case unattractive.

Compliance costs can be either administrative in nature (e.g., new routines, processes) or operational (e.g., local storage). Many compliance costs are in fact negligible for a company the size of Ericsson. However, more cumbersome is the effect on new revenue generation and hence innovation since compliance with regulation has negative impact on innovation cycles, e.g., speed as well as market diffusion of new innovations (e.g., time to market). In a fast-moving world like ICT, delays in innovations due to conforming with data protection rules can mean losing 'first move advantage' and hence business opportunities.

7.3 Google Sweden

– “If you want to use the Internet, you must move data”

Google Sweden is a subsidiary of Google. In Stockholm, Google Sweden has a research and development office. Google Sweden also houses sellers of Google’s business solutions (e.g., Google Apps). However, they only function as a link between the customers and Google’s sales office in Ireland. Google Sweden does not have any servers in Sweden—like Google’s entire operations, everything is cloud based.

Even if Google Sweden does not actually sell anything, they handle customer data. They do not handle any user (personal) data. Issues relating to privacy and data transfers are essential elements when dealing with potential customers. Customers look at Google’s products to make their businesses more effective and develop new innovative products—and here the ability to move their own data freely across borders is essential. Hence, according to Google Sweden, barriers to data transfers threaten companies’ competitiveness.

Today, Google’s customers also rely on unfettered data transfers to receive updates and new services to all their facilities around the world at the same time. Virus or other security threats to customers’ data systems can be remedied directly globally (instead of region by region) with the help of international data transfers. Finally, customers’ mobility increases by allowing speedy access to company resources anywhere in the world. Any restrictions on data transfers jeopardise these benefits.

Some of the current legislation in Europe on privacy creates problems for Google Sweden when dealing with customers. For example, it is common for companies like Google (and many other companies in all economic fields) to use subcontractors for different tasks relating to their data processing, for example, for troubleshooting or technical support services. The needs of customers to control their data—and hence know all companies that might process their data—might conflict with Google’s need to ensure secure data handling. A like problem is auditing, where customers have the right to audit the facilities where data is stored. Two difficulties arise: one is that, for security reasons, Google does not want to grant access to

server halls,¹¹¹ the other is the fact that all data transferred to Google is divided into several parts that are in turn spread to multiple data centres. Hence, the traditional view of data as having a single location is not valid.

The R&D unit at Google Sweden relies on data transfers to jointly work with other units around the world. The entire process builds on open systems where data can flow freely. So far, Google Sweden has not experienced any problems with regard to privacy. However, they are mindful of any regulatory developments that would, as they put it, ‘balkanize the Internet’. This would cripple innovation and slow down spreading new solutions to users.

7.4 Hermes Medical

– transferring data for medical and scientific purposes

Hermes Medical Solutions was established in Stockholm, Sweden in 1976 (formerly Nuclear Diagnostics). Hermes Medical Solutions is a leading manufacturer of software applications in molecular medical imaging used in processing and display from different modalities¹¹² such as CT, PET, SPECT, MRI, DX, and QUS. The company also develops and markets PACS¹¹³ solutions for storage, archiving, and management of medical images. Hermes Medical Solutions develops applications in several areas such as cardiology (dynamic applications), kidney, and liver, as well as advanced solutions in oncology from the location of the tumor to radiation therapy planning.

All of the applications are also available as cloud based solutions, where customers can perform the same tasks and share the medical images with other departments and centres. The customers’ are hospitals and pharmaceutical companies in 30 countries (about 2000 users), either with equipment installed on their premises or, more commonly, through cloud solutions. Hermes Medical Solutions has subsidiaries and affiliates in Sweden (HQ), UK, the U.S.A., Canada, and China. The different offices are separate companies and hence no HR data needs to be transferred. It is handled locally.

The services offered by Hermes Medical Solutions are based on digitilised images and 95 per cent of Hermes services are ‘remote’. All patient



data is stored in servers in Sweden, where Hermes Medical Solutions hires storage and processing space. Moreover, Hermes Medical Solutions take part in different scientific projects, including a project with over 200 hospitals that upload data about a specific illness on Hermes Medical's servers. These images can be shared between participating actors. The system is used for clinical studies and here data transfers are a necessity. Another example is an EU-financed project involving 234 hospitals in 20 countries. All this requires data transfers—both to and from Sweden but also between different hospitals and scientists through Hermes' system.

Regarding data protection laws, Hermes Medical has contracts with users stating that the users own the data (they are data controllers) and Hermes administers it. Hermes Medical is a covered entity. It is for the Data Controller to ensure that data can be transferred to Sweden and, in some instances, shared. A problem for Hermes Medical is that many hospitals do not have enough knowledge about their national legislation. But, generally, since Hermes Medical Solutions does not own the data, they have not had any specific problems with data regulation. They are, nevertheless, conscious about local storage requirements. Such rules in small countries (like Denmark) would force Hermes out of these countries since the costs would be too high to set up separate installations.

The challenge for Hermes Medical is to ensure that their system is secure enough so customers can use their system without breaking their national legislation. Adapting can also involve costs. The system must be fast and safe from leakage.

A potential problem is if something goes wrong, where the company is required to report incidents,

for example, in accordance with the vigilance procedures in the European Medical Device Directive¹¹⁴ and the Medical Device Reporting procedures in the United States.¹¹⁵ In both cases, demands that data must be sent to both the EU and the U.S.A. This includes unaltered data, which can include private information (patient's name, for example).

7.5 HL Display – data transfers allow the bumble bee to fly

HL Display manufactures and sells product displays for stores. This includes designing and providing the entire interior of shops. They are world leaders in their field with customers and sales offices in 48 countries. HQ is in Nacka, Sweden. 1,200 people work HL Display. Manufacturing and logistics centres are in Sweden, Poland, UK, and China.

HL Display titles themselves 'the bumble bee that can fly' and IT solutions and data transfers are what give them air under their wings. Given their small size, they should not be as successful as they are but effective processes based on digital solutions allow them to be competitive. With digital, mainly cloud-based solutions, all information is accessible to all employees (including salespeople in the field) instantaneously. If data is compartmentalised and stored in different places, employees might not have access to the right data at the right time.

For HL Display, cloud solutions are more efficient and preferable for ensuring global access. Cloud solutions also allowed HL Display to set up an IT department in Poland, a solution that would



have been too expensive without the cloud. The problem is that HL Display's data contains some sensitive information like user accounts. This affects how the company can handle their data in the cloud. Using a cloud provider with servers in the EU solves parts of the problem since this allows for free circulation of sensitive data within the EU.

Privacy regulations have affected HL Display's business in several ways. One solution they offer to customers is video screens in the stores for product presentations. The service is based on a content management system driven by Amazon. This is a cloud solution offered to the store owner.

HL Display is contemplating moving their HR system to a cloud solution. Today salary and other like systems are local. In at least one large market, there are restrictions on moving such data out of the country. This will necessitate building a separate system to handle this restriction.

Censorship is a concern. The manufacturing plant in China has a separate server that is not easily accessible from abroad. The national firewall creates lags and might interrupt transfers. Data is thus hindered from flowing freely within HL Display's system. Censorship developments in some other countries might pose similar problems.

HL Display is troubled by different standards between ICT suppliers, and the development of data flows might be hampered by this. Standards help companies speak the same language—both in-house and with third parties.

'Internet and communication is as important to HL Display as roads are for car salesmen – and soon even more important.'

7.6 Klarna – regulatory patchwork hampers trade possibilities

Klarna offers on-line payment solutions and is head-quartered in Stockholm, Sweden. It operates in seven European countries, serves 18 000 stores and 12 million customers. Klarna has a R&D-office in Israel. Its central data base is located in Sweden.

Klarna's services are Internet based and, being the facilitator between on-line seller and buyer, Klarna's services rest upon the possibility of moving digitalized information about the parties of the transaction. Klarna handles three types of data; i) corporate data, including HR-data, ii) end-customer data (B2C-data) and iii) merchant data (B2B-data).

Klarna's business is dependent on moving data across borders, including data needed to identify the customer and making credit reports. Having an R&D-office in Israel entails allowing remote access to data in Sweden in order to improve existing services and develop new services. Finally, Klarna tries to combat fraud by analysing customer data. A final example is that Klarna, like most companies operating in different countries, needs to move employee data to the HQ in Stockholm.

For Klarna, restrictions on data transfers – not at least the existence of different levels of protection in different EU-member states – risk impeding business. Restrictions entail appliance costs (e.g. three lawyers work full time with data protection issues), aggravated product development and expansion into new markets may be effected. In fact, cumbersome personal information regulations have in the past been one of the reasons that lead Klarna to refraining from entering a new market. Furthermore, complex and differing local data protection regulations, poses challenges also to partnership and cooperation, as this gives rise to cumbersome differences and negotiation challenges towards partners, vendors etc.

For historic reasons, most problems has related to regulations in European countries. Nevertheless, Klarna finds U.S. legislation problematic as well, and, lately, the varying information on the applicability of the Safe Harbour framework for instance. A specific U.S.-concern relates also to OFAC (Office of Foreign Assets Control) and the demand on financial companies to do terrorist screening – a demand that is not compatible with Swedish regu-

lation on data protection¹¹⁶. In general, the rapidly changing technological environment poses challenges for international cooperation, as cooperating with service suppliers from outside the EU usually is very time consuming. Compliance requirements vary and complex services are many times depending on some kind of data sharing or transfer, which often is difficult to achieve taking into consideration differing data transfer requirements.

EU-regulation restricts Klarna sometimes from processing data where they would like. In addition, they are sometimes hindered from using cloud services to share data with for instance service providers or between offices in different countries. This is since using cloud services automatically entails a transfer of data. Klarna finds that data transfer regulation affects product development since the R&D-office only can get limited access to Klarna's data and it is unpredictable what kind of data they are allowed to access. All access equals transfer of the data outside EU. Klarna have at times solved this by moving persons (including family) to Sweden – even though this is more costly.

Finally, Klarna considers that the overall uncertainties about the new draft EU regulation, what the final text will look like and when it might be decided and come into effect, poses a great challenge. Klarna is committed to integrity and data protection considerations, doing its utmost to consider these issues already in development (“Privacy By Design”). The uncertainties however make this a challenge as the structuring of the processing activities sometimes are long-term solutions that may take time to change. According to Klarna, a revamp of the data protection framework is vital, but in order to enable proper planning and making business able to foresee how to proceed, it is important that it does not take too long before an EU decision is made regarding the new framework.

7.7 NASDAQ OMX Stockholm – Safe Harbour simplify data transfers

NASDAQ OMX Stockholm (NOMX) is a subsidiary of the U.S.-based mother company—a stock exchange company. In Stockholm, NOMX has approximately 750 employees out of which about

500 are engineers and computer experts. This is due to the fact that NASDAQ's R&D unit is situated in Stockholm. NOMX has data servers in Sweden.

NOMX's business is divided into four activities: market data (data transactions, which are packet and sold to customers), transactions, technology, and listings. Market data and listings do not involve personal data while the other two do. Nevertheless, all four activities demand transferring and processing large amounts of data.

Technology is the activity most affected by data protection regulations. NOMX run over 70 stock exchanges from 50 countries, including third party exchanges. Customers seeking NOMX's services are concerned about data handling and server placement. To abide by EU regulations and customer needs, NOMX have servers in the EU. Preferably, NOMX would like to have run all from one place, which is the mother company, to ensure full efficiency and avoid compliance costs. This also includes some added-value services offered by NOMX.¹¹⁷ Nevertheless, since many customers find value in it, there is an advantage to offering servers placed in the same regulatory environment as the customers.

NOMX consider themselves a technology supplier and all data are customers' data running in NOMX's systems. For NOMX, it is essential that customers are responsible for their own data and this is taken care of contractually.

Like most subsidiaries, NOMX need to move HR data to their mother company. To this end, NOMX have used the Safe Harbour principles. It has worked very well for them.

7.8 Readsoft – using an American global supplier ensures security requirements for the cloud

ReadSoft offers software solutions for document process automation on premise or in the cloud. ReadSoft has 600+ employees, in 17 countries all around the world, serving over 10000+ customers (including some world leading companies).

ReadSoft's solutions are based on digitising and processing documents, and extracting information from business documents such as invoices, forms, claims, and orders. The information is used, for example, to automate document sorting and infor-

mation matching against enterprise resource planning systems. Some processes involve data transfers to and from ReadSoft's servers located in various locations (using Microsoft as server supplier). ReadSoft uses several cloud solutions—both to handle their internal data (including HR data) and as part of their services to customers.

Besides HR data and data in customer relation management (CRM) systems, ReadSoft handles mainly business information. Hence, ReadSoft has not experienced any particular problems concerning, e.g., data protection regulations. ReadSoft is rolling out a new e-invoicing systems and in this process they have consulted a third party specialising in compliance issues in order to ensure tax and legal compliance.

Fundamental for ReadSoft is that they can build systems guaranteeing no unauthorised access to customers' data, that data is not corrupted and that it is accessible without delays. ReadSoft believes that using an American global supplier ensures questions about security, data protection, privacy, and data ownership are answered because of its built-in capabilities for compliance with a wide range of regulations and privacy mandates.

ReadSoft observes that companies' practices differ from one country to another. Especially German customers are more concerned about data leaving Germany and have higher demands concerning content and security than companies in other European countries. This implies adaptation costs for ReadSoft.

ReadSoft are aware of possible restrictions on moving their customers' data based on legal requirements or customer demands. This would require building local customised solutions and abandoning global cloud solutions. This would mean higher prices, a need to abandon smaller markets and the inability to upgrade services to all customers at the same time.

7.9 Scania – using data in trucks has reached point of no return

Scania is a global company offering, in their words, 'sustainable transport solutions' with a focus on trucks, buses, and engines. They offer products, services, and financial solutions to their customers. Scania is a global company with a sales and service organisation in over 100 countries. Nearly 40,000

are employed by Scania. HQ is in Södertälje, Sweden, where also R&D, production, purchasing, sales, and IT systems are situated. Scania also has production sites in Brazil, Netherlands, Argentina, France, and Poland as well as regional production centres in six other countries (all outside the EU).

Data is sent between all the units that form a part of Scania, including to franchisees. Most data relate to products. This includes data from products in use as all vehicles are connected to the Internet and transmit anonymous performance data. This data is used for analysis and testing. Only a small part of transferred data is related to personal data.

The use of data has passed 'the point of no return'. Vehicles would not function effectively without transferring data, and neither would repairs. If a vehicle brakes down, data can be transferred to a regional or global help desk for help in tracking and solving the problem. The 'old repair manual is replaced by a global data base' and hence effective repairs hinges on data transfers.

A service offered by Scania is an educational service called 'ecolution'. Scania measures how a driver drives his vehicle, packages the information, and sells the knowledge to the driver and his employer. The purpose is to continuously coach the driver on how to operate the vehicle in a more efficient and environmentally friendly way. The service is operated from Sweden and involves the transfer of personal data, which is the driver's data. Scania has put a lot of effort into ensuring compliance with local personal data protection laws. So far, Scania has not experienced local storage demands but such rules would make the service unprofitable in smaller markets.

When it comes to R&D, approximately 90% of it is done internally. In some instances subcontractors are used, but Scania takes care to ensure that personal data is not accessible. Data protection regulations have slowed down development sometimes but never hindered it.

Personal data is mostly connected to employees and more or less contained to internal processes. Some tools include sensitive HR data, for example, job application and competence databases. Scania works with individual acceptance in each situations where personal data might be transferred. This gives employees control and knowledge about how their data is handled. The downside is the cost of building a system with many authorisations.

To handle issues relating to data transfers and personal data, Scania has established a 'privacy forum'. Here, representatives from the legal, HR, and IT departments meet to discuss privacy and how Scania's operations and processes must be adapted to fulfill privacy requirements.

Whistleblower programmes¹⁸ are an important element for Scania to ensure high ethical standards. Here, data protection regulations become cumbersome since they require consent from national data inspection boards.

On data protection regulation generally, Scania would like to see clearer rules and harmonisation. Uncertainties lead to hesitations of sharing data. On a positive note, data protection regulations have led to an environment where Scania restricts gathering personal data to what is strictly necessary.

Scania's servers are situated in Södertälje. The company has been hesitant to outsource parts of the IT systems to cloud providers and has not been willing to 'let go of control'. Nevertheless, the back office system will soon be outsourced to a multinational firm with servers in India.

7.10 Swedbank – bank services involving enormous data transfer needs

Swedbank's main business is in Sweden and headquarters are in Stockholm. The company also has affiliates in the Baltics and Luxembourg, branches in the U.S.A., Denmark, Norway, Finland, and China, and a representative office in Spain. The bank has 7.8 million private customers and more than 600,000 corporate and organisational customers.

The banking business is all about processing and transferring data. A lot of data is transferred within the Swedbank Group but financial transactions also demand the transfer of data, including clearing, payments, fund investments, etc., to third parties, e.g., cooperation parties. All transactions need back-up and subsequently double the storage of data. Internet banking is also an activity based on moving data. In relation to processing personal data, bulk purchases of stocks by the Group do not cause concerns in relation to data protection. However, lower levels of purchases (e.g., for individual

people) necessitate a large amount of personal data to be transferred. Some HR data also needs to be moved and processed. This results in a large amount of processing of personal data.

Swedbank Group aims to centralise its IT operations, e.g., maintenance and development, to create synergies and cost efficiency. Swedbank Group has centralised data centres in Estonia and Sweden and data from the banks within the Group could be stored in Estonia or Sweden. The banks within the Group are also outsourcing some IT operations both internally and to third parties. A small part of IT development is outsourced to India (no processing of personal data). Outsourcing entails data to be shared.

Generally, Swedbank sees transferring data within the EU/EES as rather unproblematic. However, a recent law in Estonia demanding that continuous operation of vital services (financial transactions and withdrawals) must be maintained within Estonia has led to cost increases due to the need for double operations (both in Estonia and Sweden).

Swedbank finds the U.S. legislation to some extent difficult to handle. Since EU legislation or advice is not recognised in the U.S, the bank is not allowed to give advice to customers residing in the U.S, not even general stock advice on its own homepage. Since the information is put on a homepage in Sweden there is a de facto data transfer in this case. As a result, it is difficult for Swedbank to have U.S. Internet bank customers. Another concern with the U.S.A. is information required by tax authorities, the FATCA rules, which require substantial processing in a huge number of systems, which in its turn is costly and time-consuming for the Swedbank Group. Finally, the OFAC (Office of Foreign Assets Control) demands on financial companies to do terrorist screening may conflict with Swedish privacy regulations.

Cloud services are a new field that enables data transfer and personal data processing worldwide. When the Data Protection Directive was decided more than ten years ago, there were not any cloud services. The global suppliers use very standardised contracts that are not fully compatible with EU legislation and it is rather difficult for the data controller to be compliant with the legislation. Customer support, which is moved around the world based on the time of day, is especially cumbersome as Swedbank must know where personal



data is processed, who the subcontractors are and how they guarantee the safety of the data. It is very much a contractual issue but EU legislation adds a layer of complexity by being, in the eyes of the suppliers, too stringent.

As a financial institution, Swedbank is used to handling strict legal demands. Privacy regulation as such is not a concern—but it should be harmonised. In addition, clearer rules to guarantee security are welcomed.

7.11 Tele2 – M2M-services cannot be developed and utilised optimally

Tele2 is a telecom operator with 15 million customers in 10 countries (9 in EU/EEA and in Kazakhstan). The company has 7,500 employees. Tele2 offers mobile services, fixed broadband and telephony, data network services, cable TV, and content services. Hardware, such as routers and TV boxes, are mainly produced outside the EU and configurations are often developed and performed in a collaborative way. A lot of software development is also performed outside the EU or in close collaboration with developers outside EU.

Being a telecom operator, the entire business of Tele2 is about transferring data. This includes everything from the actual connection of telephones and charging for their services to marketing, customer support, and positioning. Content

services are delivered electronically as well as TV programs—all of which are data transfers. Data transfers are also included in developing new services, including with 3rd parties. Finally, being an international company, HR data needs to be transferred.

Tele2, like all telecom operators, handle a large amount of personal data of different sorts. This includes phone- and IP-numbers, data about customers (addresses, etc.), location of mobile phones, customers' content data (what they themselves transfer), etc. Due to this specific position, telecom operators are governed by more restrictive rules than other companies, notably the ePrivacy directive.¹¹⁹

One problem for Tele2 is that non-telecom operators supplying telecom services (e.g., video or voice-over-Internet services) do not have to follow the same rules when providing equivalent services as those from telecom operators (namely the ePrivacy directive does not apply to them). This creates uncertainty for end-users but also provides an imbalance in competition.¹²⁰ Another problem is that the Safe Harbour agreement does not cover the demands of the directive. Thus, there is a need for additional negotiations on clauses to safeguard the ePrivacy rules, which also means that these clauses and practices may vary on these matters between operators. A level playing field is essential to ensure fair competition between different actors.

Tele2 are involved in developing and running machine-to-machine (M2M) services. M2M services, like all 'Internet-of-Things' solutions, are

entirely based on the ability to send data. Consent from vehicle owners is needed when the data Tele2 has access to is seen as personal data and used commercially (e.g., marketing, customer support, improving the service itself)¹²¹ and when private data is transferred outside the EU. Without consent, or high costs acquiring consent, Tele2 cannot process data to develop and deliver new services. If data could be transferred to companies in third countries that can guarantee that they fulfill the requirements in the EU, it would facilitate product development. Today, R&D departments cannot have access to all relevant data.

A hypothetical example—say that Tele2 is working with a vehicle manufacturer to connect vehicles to the Internet¹²² and to have information about their geographical location sent to Tele2—and, when needed, to other companies—to analyse data (e.g., directly to a tow truck in case of a break down). When deciding how to set up such services, Tele2 would have to see if the software providers are within the EU or outside. If the providers are outside, it may be difficult to use them—even if their service is better. Data laws mean that Tele2 could not always collaborate with preferred companies and both Tele2 and the vehicle manufacturer would need to acquire consent from the car owners in order to transfer data. Third parties wanting to use the data meet the same problem.¹²³

Another concrete example is the introduction of a payment system (a new service) in nine European countries. This entails analysing privacy regulations, including how consent must be gathered, how data can be stored, and which parts of the data Tele2 is allowed to process. For Tele2, it is important to launch the payment service in all countries simultaneously and ensuring compliance is costly for them and affects innovation. Harmonisation of the rules on data protection would have facilitated the process.

For Tele2, local storage requirements have posed problems, including the need to leave a country. In this case, consent from governmental authorities was needed to transfer all types of data out of the country. The company had to build separate data systems to handle this requirement—at a very high cost. In Norway and Estonia, all data retention information (information that can be connected to serious crime, e.g., IP and billing addresses) needs to be stored in the country. According to Tele2, the separate storing facilities led to increased costs.

Beyond their own concerns, Tele2 highlighted the fact that in Sweden there are about 570 telecom operators, half of whom are required by data retention laws to store their data. More and more companies use third-party storage suppliers to handle this, usually cloud suppliers due to cost reasons. How is data secured in these cases?

7.12 TeliaSonera – looking for more restrictive Safe Harbour principles

TeliaSonera is a telecom operator partly owned by the Swedish and Finnish governments. It has 183 million customers in 29 countries. The company operates a wholly owned global fiber network and is part owner of the transatlantic fiber optic cable. TeliaSonera offers a broad range of services, including mobile services, fixed broadband and telephony, data network services, cable TV, and content services. In addition, they provide cross-border wholesale services (i.e. IP, capacity, and colocation services as well as international voice interconnect services) for both domestic and international customers. HQ is in Stockholm, Sweden. TeliaSonera employs 26,800 people in offices around the world.

TeliaSonera summarised their data transfer needs with respect to customer data (including call specifications, data about the client, traffic data, and localisation) and HR data. In addition, TeliaSonera has outsourced some services to companies which have affiliates located outside the EU. This would include services like fault handling.

HR data handling for employees is predominantly centralised in Sweden or Finland. The transfer and handling of employee data have to fulfill local country requirements. In some cases, the employee needs to consent to the data being transferred to another country as well as being handled in another country. In some countries, there are other requirements as well—for example, in Germany where consent has to include the country where the server is located.

By and large, TeliaSonera did not have any major problems with data transfer issues. The problem is instead keeping up with the various different local variations when it comes to data protection and the transfer of personal data, creating compliance costs. Even within the EU, member states have local dif-

ferences that have to be reviewed and fulfilled. And compared to other countries outside the EU, the differences are even greater. The review and implementation of the local variations are time consuming and an administrative burden that generate substantial costs.

On a more specific level, telecommunication services are vital to society and their services have to work even during war, and thus the system needs to be within the country's borders in order to be able to operate. Such consideration leads to TeliaSonera having to build local networks for core services (e.g., telephony and SMS). This amounts to increased costs.

TeliaSonera uses Safe Harbour in their dealings with the U.S.A. While basically approving the system, TeliaSonera consider it to have some flaws, such as lack of transparency and the fact that companies must themselves ensure that U.S.-based companies fulfill the demands. A certification system that removed the need to inspect U.S.-based companies would be welcomed. Currently, the system is administratively costly and time consuming. TeliaSonera also found the Safe Harbour principles to be too relaxed, especially with regard to new and inexperienced companies. Today, it can be hard to negotiate data protection with these companies and higher standards in Safe Harbour would facilitate this.

Finally, TeliaSonera finds Turkey problematic since national laws obstruct coordination of tasks. The result was a need to put more IT systems in place in Turkey and find new ways to coordinate operations in Turkey with the rest of the world.

7.13 TrustWeaver – compliance would equal unfeasible administrative burden

TrustWeaver is a small company (25 employees) in Stockholm, Sweden, offering business transaction compliance services including e-signing and archiving for e-invoices. TrustWeaver ensures compliance with local integrity and authenticity requirements in 47 jurisdictions, i.e., guaranteeing that e-invoices (and other e-documents) are recognised as authentic and unchanged by both courts and authorities in these countries. TrustWeaver provides hundreds of the largest companies in the

world with services to make their business transactions compliant.

The entire business model is digital and with invoices going to and from 47 different countries, data transfers are obviously essential elements. For the EU, American, and many Asian countries, TrustWeaver process the invoices and have their archives in Sweden. However, for TrustWeaver's service provision in Latin American countries, European privacy legislation becomes a hurdle. In these countries, e-invoices must be processed, signed, and often stored locally. To meet these requirements, TrustWeaver works with local sub-contractors to whom the invoices—and the personal data (normally of Latin American citizens) they may contain—are transferred.

The European Commission has for such transfers issued *Standard Contractual Clauses*,¹²⁴ which need to be in place to allow personal data to be exported from the EU. These Standard Contractual Clauses are drafted for the data *controller* and a non-EU *processor*. However, since TrustWeaver is an EU processor using a non-EU *sub-processor*, these Standard Contractual Clauses can only be used between TrustWeaver and the sub-processor if TrustWeaver is given a clear mandate from every EU controller to enter into the clauses 'in name and on behalf' of the EU controller.

The crux is that with hundreds of thousands of controllers, this is administratively unfeasible. The personal information in the invoice is usually just reference names within the trading partners' organisations, which will normally not have a contractual relationship with the controller or processors. Hence, the reference person cannot consent to the transfer.¹²⁵ According to TrustWeaver, most companies and authorities do not seem to be aware that a reference person's name in an invoice would be covered by data protection regulation in the EU—or they turn a blind eye to the problem.

'When things get too complex and it becomes too burdensome to comply, companies opt to not follow the law – everybody sends invoices and everybody has to deal with invoices containing personal data, but very few organisations comply with the law.'

Today, TrustWeaver's servers are located in Sweden. However, in the future, the company may be looking towards cloud solutions. Unfortunately,

cloud solutions bring forth new problems. One is that a cloud service provider can guarantee that servers are located in Europe but still have contracts stipulating that the data can be moved to, for example, the U.S.A. or India for troubleshooting and other technical services, thereby making the 'localisation' of the service futile (since, in the end, data might still be moved). The legal benefit of using a local or regional provider to comply with EU rules is therefore gone. Another problem is that the largest cloud providers are American and clients are wary about what the U.S. government can demand access to.

7.14 Volvo – data is a key asset that must be kept safe

The Volvo Group manufactures trucks, buses, construction equipment, and marine and industrial engines, and also offers financing and service solutions. The Volvo Group employs some 115,000 people, has production facilities in 19 countries, and sells its products in more than 190 markets. The headquarters is in Göteborg, Sweden.

The business model is built on digital solutions. Volvo's products are digitised and, e.g., information sent from trucks in operation is used to help customers with optimising cargo loading, fuel efficiency, etc. Vehicles can be monitored in real time to see how they are performing and whether repairs or software upgrades are needed.

Information is a key asset for the Volvo Group: information about customers, employees, products, and their usage. Safekeeping this data is paramount and a focal point when dealing with data and data transfers. A consequence is that the Group handles much of their data by themselves, with servers in Sweden, and deems it essential to be careful with whom they share data. Some outsourcing has been done but has involved lengthy negotiations to ensure security and risk minimisation. The location of the servers is important.

Most of the Volvo Group's data transfers relate to products, product development, and production. Systems are adapted to existing legislation to not cause issues when transfers of sensitive information, e.g., HR information. Some global solutions have therefore been aligned to regional requirements to ensure compliance, but on the whole, there are no issues with compliance.

7.15 [Manufacturing Company] – going global necessary despite reduction of flexibility

This Sweden-based manufacturer operates in a global market with customers in many countries across Europe, Middle East, Africa, the Americas, and Asia.

Even being in a company working with manufacturing, digital solutions are essential elements and movement of data within the group, and to resellers, is essential. Mostly, the company transfers data related to products and customers. Chiefly, customer data does not include data related to people. However, when working on projects customising products to the specific needs of a customer, personal data can be involved. This is partly because company representatives work on a project basis within the customer's organisation. Most company data relating to people are employee data.

The company primarily use their own servers situated in Sweden. Outsourcing is limited but they are looking at outsourcing their HR system to a cloud supplier. However, information security is essential and a challenging task in a global organisation, especially for ensuring protection of personally identifiable information when outsourcing. The key is negotiating an agreement with suppliers that fits security needs.

The company is currently in period of transformation. They are moving from a business structure with local units ensuring local compliance with laws and regulations to introducing global systems. One example is the introduction of global ordering system—a system accessible to all within the group and certified resellers from anywhere at any time. The system will make operations much more efficient and the company more competitive.

Moving from local to global requires business changes all the way from preparing a business proposal to making the delivery. Like any global initiative spanning multiple countries, the business culture needs to change from fully local control local to global control. Globalisation is a necessity in order to stay competitive in the global market space. However, while on one hand reaching more openness within the entire group, on a local level globalisation brings forth a lower level of access to information (i.e. data). A key to success has been openness and internal knowledge sharing something that now has to be limited.

Literature

- Borga, Maria and Jennifer Koncz-Bruner (2012), "Trends in Digitally-Enabled Trade in Services"
- Castro, Daniel (2013a), "The Cost of Privacy: Netflix – Three Years & Three-Quarters of a Million Dollars"
- Castro, Daniel (2013b), "How Much Will PRISM Cost the U.S. Cloud Computing Industry?"
- Castro, Daniel (2013c), "The False Promise of Data Nationalism"
- Castro, Daniel and Jordan Misra (2013), "The Internet of Things"
- CCIA Europe (2013), "The Internet: the Enabling Force of the 21st Century"
- Christensen, L., A. Colciago, F. Etro and G. Rafert (2013), "The Impact of the Data Protection Regulation in the E.U."
- eBay (2012), "Towards Commerce 3.0 – Roadmap for Building Sustainable Growth into Commerce"
- eBay (2013), "Commerce 3.0 for Development – The Promise of the Global Empowerment Network"
- ECIPE (2013), "The Economic Importance of Getting Data Protection Right – Protecting Privacy, Transmitting Data, Moving Commerce"
- Ericsson (2010), "CEO to shareholders: 50 billion connections 2020"
- Erixon, Fredrik (2013), "EU Policies on Online Entrepreneurship: Conversations with U.S. Venture Capitalists"
- European Commission (2012a), "How Will the EU's Data Protection Reform Benefit Businesses?"
- European Commission (2012b), "Impact Assessment (SEC(2012) 72 final)"
- European Parliament (2012), "Data Protection Review: Impact on EU Innovation and Competitiveness"
- Ezell, Stephen (2013), "Written Testimony to the US International Trade Commission", Investigation No. 332-531, Hearing: Digital Trade in the U.S. and Global Economies"
- Ezell, Stephen J., Robert D. Atkinson and Michelle A. Wein (2013), "Localization Barriers to Trade: Threat to the Global Innovation Economy"
- Fleming, Jeremy (2013), "TTIP: Data is the elephant in the room"
- Froman, Michael (2013), "Keynote Remarks by U.S. Trade Representative Michael Froman at the World Trade Organization Public Forum on Innovation and the Global Trading System"
- Hirsch-Kreinsen, Hartmut, David Jacobson and Staffan Leastadius (eds.)(2005), "Low-tech Innovation in the Knowledge Economy"
- Hufbauer, G.C., J. Schott, C. Cimino, M. Vieiroand and E. Wada (2013), "Local Content Requirements: A Global Problem"
- Korte, Travis (2013), "Using Data to Fight Counterfeiting"
- Kroes, Neelie (2013), "Data isn't a Four-letter Word"
- Lee-Makiyama, Hosuk (2013a), "European leaders should leave data flows open"
- Lee-Makiyama, Hosuk (2013b), "A Multilateral Legal Assistance Protocol: Preventing Fragmentation and Re-territorialisation of the Internet"
- Mayer-Schönberger, Viktor and Keneth Cukier (2013), "Big Data – a revolution that will transform how we live, work, and think"
- McAfee, Andrew and Erik Brynjolfsson (2012), "Big Data: The Management Revolution"
- McKinsey Global Institute (2011), "Big Data: The Next Frontier for Innovation, Competition and Productivity"
- National Board of Trade (2011), "Survey of E-Commerce Barriers Within the EU – 20 Examples of Trade Barriers in the Digital Market"
- National Board of Trade (2012a), "Everybody is in Services – The Impact of Servicification in Manufacturing on Trade and Trade Policy"
- National Board of Trade (2012b), "How Borderless is the Cloud? – An Introduction to Cloud Computing"
- National Board of Trade (2012c), "E-commerce – New Opportunities, New Barriers"
- National Board of Trade (2013a), "Global Value Chains and Services – An Introduction"
- National Board of Trade (2013b), "Just Add Services – a case study on servicification and the agri-food sector"
- National Board of Trade (2013c), "Minecraft Brick by Brick – A Case Study of a Global Services Value Chain"

- National Board of Trade (2013d), “*Making Trade Happen*”
- OECD (2011), “*Exploring the Economics of Personal Data*”
- Ponemon Institute (2011), “*The True Cost of Compliance*”
- Robinson, Neil et al (2009), “*Review of the European Data Protection Directive*”
- Rosen, Jeffrey (2012), “*The Right to be Forgotten*”
- Stone, Susan (2013), “*Emerging Trade Policy Issues – Localisation Barriers to Trade*”
- Thierer, Adam (2013), “*A Framework for Benefit-Cost Analysis in Digital Privacy Debates*”
- UNCTAD (2009), “*Information Economy Report 2009*”
- UNCTAD (2013); “*Information Economy Report 2013 – The Cloud Economy and Developing Countries*”
- UK Ministry of Justice (2012), “*Proposal for an EU Data Protection Regulation – Impact Assessment*”
- USITC (2013), “*Digital Trade in the U.S. and Global Economies, Part 1*”
- Wakefield, Jane (2013), “*Mobile phone data redraws bus routes in Africa*”
- Winham, Ian (2013), “*Companies must reap benefits of new EU data protection rules*”
- World Bank (2012), “*There Goes Gravity – How eBay Reduces Trade Costs*”
- World Economic Forum (2011), “*Personal Data: The Emergence of a New Asset Class*”
- World Economic Forum (2012), “*Rethinking Personal Data: Strengthening Trust*”
- World Economic Forum (2013), “*Unlocking the Value of Personal Data: From Collection to Usage*”

Interviews

Company	Person(s) interviewed	Date of interview
eBuilder	Mikael Ekström, Senior Vice President Marketing	13th of June, 2013
Ericsson	Rene Summer, Director Government and Industry Relations	5th of June, 2013 plus written submission
Google Sweden	David Mothander, Sales Manager Google Enterprise Sweden Olof Hernell, Cloud Evangelist	26th of June, 2013
Hermes Medical	Jan Bertling, CEO & President Joakim Arwidson, Quality Manager	28th of Aug., 2013
HL Display	Chief Architect and Infra Manager Ola Hesselroth	13th of July, 2013
Klarna	Caroline Olstedt Carlström, Chief Counsel Global Data Protection Claes Tellman, Head of Communications	19th of June, 2013
NASDAQ OMX	Magnus Billing, President NASDAQ OMX Stockholm, Transaction Services Nordic	20th of Sept., 2013
Readsoft	Patrik Fältman, Business Line Manager P2P Julius Eyem, Director of Operations	30th of Aug., 2013
Scania	Niklas Jedeur-Palmgren, Head of Management System - Global Support	29th of Aug., 2013
Swedbank	Pia Wrakhuvud, Compliance Officer	13th of July, 2013
Tele2	Michaela Angonious, Head of Regulatory Affairs Mikael Alenmark, Corporate Responsibility and Data Protection Officer	4th of July, 2013
TeliaSonera	Ann Ekstrand, Corporate Counsel Mattias Karlsson, Corporate Counsel Sarah Modigh Engström, Legal Counsel Peter Lav, General Counsel TeliaSonera International Carrier Jan Wellergård, Security Director Group IT	4th of Sept., 2013
Trustweaver	Anna Nordén, General Counsel	25th of Sept., 2013
Volvo	Krister Eliasson, Senior Vice President Process and IT Efficiency	2nd of Sept., 2013
[Manufacturing company]	[Anonymous], Chief Information Security Officer	27th of Aug., 2013

Notes

- 1 Ezell (2013)
- 2 McAfee and Brynjolfsson (2012)
- 3 National Board of Trade (2012a) and (2013b)
- 4 National Board of Trade (2013a)
- 5 This definition, taken from the UK Data Protection Act, is fitting for this study. It is not a dictionary definition.
- 6 Definition based on Directive 95/46/EC and OECD Privacy Guidelines.
- 7 WEF (2011)
- 8 OECD (2011)
- 9 See also Robinson et al (2009).
- 10 OECD (2011)
- 11 WEF (2011)
- 12 UNCTAD (2009). For the U.S.A., it is 60 per cent (Borga and Koncz-Bruner, 2012) while it is slightly below 50 per cent for Sweden (own calculation).
- 13 ECIPE (2013)
- 14 Internet-based trade increases trust and availability of information and subsequently reduces trade costs. World Bank (2012)
- 15 WEF (2013)
- 16 This is exemplified in many of the cases in the annex.
- 17 See e.g. McKinsey Global Institute (2011) exhibit 8 about data in different sectors of the economy.
- 18 European Parliament (2012)
- 19 CCIA Europe (2013)
- 20 See eBay (2012) and (2013) on the importance of digital market places for small companies.
- 21 National Board of Trade (2013a)
- 22 See National Board of Trade (2013c) for an example of a global services value chain, wholly based on digital solutions.
- 23 WEF (2012)
- 24 For example, in the Ivory Coast, localisation data from mobile phones was used to redraw bus routes. Wakefield (2013)
- 25 Quote from Meglena Kuneva, former Commissioner for Consumer Protection of the EU, in WEF (2011)
- 26 For example, buying a product on a website will entail the transfer of personal data like name, delivery and billing addresses, financial information, etc.
- 27 National Board of Trade (2012b)
- 28 European Parliament (2012)
- 29 McKinsey Global Institute (2011)
- 30 For a large number of examples of how IoT can help making environmental protection, transportation, communication, agriculture, public safety etc. more efficient see Castro and Misra (2013).
- 31 McKinsey Global Institute (2011)
- 32 Ericsson (2010)
- 33 McKinsey Global Institute (2011)
- 34 See e.g. USITC (2013) and European Parliament (2012)
- 35 See e.g. National Board of Trade (2012c) and USITC (2013) for discussion on these issues.
- 36 This chapter is based on Ezell, Atkinson and Wein (2013) and Ezell (2013).
- 37 Stone (2103)
- 38 According to Ezell, Atkinson and Wein (2013) this argument is flawed as it is based on the presumption that data is more secure just because it is being stored or processed in one's own country. They go on to say that 'just as money is more secure in established banks, data are likely more secure in large established cloud providers who are global in scope'. The authors moreover claim that the argument about jurisdiction and legal enforcement also is weak: 'governments and authorities still have legal jurisdiction over the companies who own the data, regardless of where their data are actually stored'.
- 39 Hufbauer et al. (2013)
- 40 Largely about their communications by phone and over the Internet.
- 41 The European Commission is aware that the Greek law 'has an economic effect on these [telecommunication] providers regarding and limits their freedom to organise their business' and that it will take appropriate actions deemed necessary. Ezell, Atkinson and Wein (2013)
- 42 There are exceptions, like in cases of consent, for territories with adequate protection and under Safe Harbour and like solutions (see chapter 4.3.3).
- 43 In order to provide investigative authorities with ready access to encrypted data in their servers.
- 44 UNCTAD (2013)
- 45 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- 46 The Directive is applicable in the entire EEA area.
- 47 Robinson et al. (2009)
- 48 Andorra, Argentina, Canada, Guernsey, Israel, Jersey, New Zealand, Switzerland, the Faroe Islands, the Isle of Man, and Uruguay.
- 49 This can be compared with the APEC Privacy Framework (from 2004). This framework is based on nine high-level principles governing personal data. It is an approach that allows companies from a group of countries with common values but divergent policy frameworks to transfer data within the group. As for third country transfers, it can be done to countries with generally compatible privacy

- regimes. This includes Argentina, Australia, Canada, the EU, Japan, Korea, Malaysia, Mexico, Russia, Singapore, and the U.S.A. (USITC 2013). Hence, data from APEC can be sent to the EU but not the other direction. APEC does not have the same strict approach to adequate protection as the EU.
- 50 The Commission has estimated that the variation in data protection laws across the EU costs European firms an estimated €2.3 billion each year. EU Commission (2012a)
- 51 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – COM(2012) 11final
- 52 See Lee-Makiyama (2013b) for discussion on extra-territorial application.
- 53 Christensen et. al. (2013)
- 54 As laid down in article 17 of the proposed act.
- 55 See more about effects in ECIPE (2013) and Rosen (2012)
- 56 In the U.S.A., the term 'privacy protection' is more commonly used—based on the presumption that only private information can be protected. In the EU, the term 'data protection' is used to indicate that it can cover information in the public domain. USITC (2013)
- 57 Other countries with sectoral approaches include Brazil, Dubai, Greenland, India, Singapore, Thailand, and Zimbabwe (USITC 2013).
- 58 European Parliament (2012)
- 59 European Parliament (2012)
- 60 ECIPE (2013)
- 61 European Commission (2012b)
- 62 All references in this chapter are found in the list of companies interviewed under "References" (if not otherwise stated).
- 63 For a further discussion of the need to attract skills, see National Board of Trade (2013c) and (2013d).
- 64 Any problem based on companies' misinterpretation of current and future data protection regulation is their own.
- 65 See e.g. Fleming (2013).
- 66 Hirsch-Kreinsen, Jacobson and Leastadius (eds.)(2005)
- 67 Summer (2013)
- 68 The issue is more about how stern protection should be, what should be protected, and how it affects business. No company argues that data protection should be done away with. Rather a balance between legitimate protection of sensitive data and the needs of businesses should be found.
- 69 Even a phone call amounts to the transfer of data – both by technically making the conversation happen and the conversation in itself.
- 70 Thierer (2013) discusses how strict EU-legislation affects among other things the effects of advertising.
- 71 This is written from the point of view of the interviewed companies (being EU based). However, strict regulations can ensure increased trust and hence also be a benefit.
- 72 For other examples of this see Robinson et al. (2009).
- 73 In some countries, certain data, like national identification numbers, cannot be moved across borders. Hence, companies cannot use this basic identification method to identify customers and must rely on less secure factors like name and address.
- 74 European Parliament (2012)
- 75 The future availability of these measures is currently debated. ECIPE (2013)
- 76 ECIPE (2013)
- 77 Summer (2013)
- 78 Many companies use this method, i.e., boxes on websites that customers or employees tick to verify that they have understood the handling of personal data and accept that this data can be processed and moved. One company uses individual acceptance every single time personal data is involved. While ensuring compliance and giving individuals control over their data, it is a costly system.
- 79 To compare, Netflix spent three years and three-quarters of a million dollar on getting privacy right on their service "Netflix social" (basically, a Facebook feature where friends can see what you have watched). Castro (2013b)
- 80 This is based on the length of time it takes to read these policies and the monetary value of that time. Example reproduced in Robinson et al. (2009).
- 81 Ponemon (2011). Costs vary substantially between industry sectors with the cost for the energy sector being almost four times as large as for the education sector.
- 82 UK Ministry of Justice (2012)
- 83 Christensen et al. (2013). In the summary, they write 'compliance with these new rules will impose a number of costs on SMEs including the need to hire additional personnel, purchase new IT software, and consult with data protection authorities in advance of certain new projects. Furthermore, rules limiting the use of personal information, particularly in advertising, will impact all businesses engaged in targeted consumer marketing.'
- 84 Note that no common EU DPA will be created. However, companies should only need to approach one DPA, hence the effect is still positive.
- 85 See also Robinson et al. (2009) and, on different response times in different EU member states, European Parliament (2012).
- 86 See also Ezell, Atkinson and Wein (2013).
- 87 Ezell, Atkinson and Wein (2013)
- 88 European Commission (2012b) and Hirsch-Kreinsen, Jacobson and Leastadius (eds.) (2005)

- 89 Hirsch-Kreinsen, Jacobson and Leastadius (eds.) (2005)
- 90 Confirmed in, e.g., USITC (2013) and European Parliament (2012). Nevertheless, one has to recognise the difference between being forced to store data in the EU (and move it, more or less, freely within the Union) and to store it in a single country.
- 91 Quite naturally, that is of less importance since the EU is the largest market for most of the companies interviewed.
- 92 Interestingly, full harmonisation would not mean that all EU-markets are the same. Several companies highlighted that all differences would not be done away with. Cultural and local (language etc.) differences would remain and still lead to different demands from clients in different countries.
- 93 Kroes (2013)
- 94 See USITC (2013) for U.S. companies' views.
- 95 More on this in Ezell, Atkinson and Wein (2013).
- 96 Oftentimes, this has to do with the need to move transferred data to third parties for, for example, trouble shooting and support 24/7.
- 97 Castro (2013b) states that the U.S. cloud computing industry could lose between \$22 to \$35 million by 2016 due to, among other, the use of the Patriot Act.
- 98 Programmes in place to expose misconduct and alleged dishonest or illegal activity occurring in an organisation.
- 99 Winham (2013)
- 100 Erixon (2013)
- 101 Note that this study has, at times, equated data protection regulation with barriers to moving data. However, as chapter 5 and the annex show other aspects of data protection regulations might create obstacles as well.
- 102 National Board of Trade (2012a)
- 103 All references are found in the list of companies interviewed under "References" (if not otherwise stated).
- 104 A value network is multienterprise and spans over the industries of the numerous e-commerce partners that participate in an end-to-end collaboration.
- 105 Business Process as a Service, BPaaS, according to the common definition of the 'cloud stack'.
- 106 Processes relate, for example, to the following businesses: Travel & Travel Expenses, Procurement, Supply Chain Management, and Financial Transactions.
- 107 Like transport companies, warehouse suppliers, repair partners, travel agencies, banks or, for example, credit card companies.
- 108 For eBuilder, the lag is small and has no practical effect, but for other companies the effect might be larger.
- 109 Ericsson holds more than 33 000 global patents.
- 110 Typically, incumbent, usually national firms that already operate in the market can thus benefit from entry barriers which also limit competition in the domestic market.
- 111 With over five million customers, that would be an uncontrollable amount of people with the legal right to access the premises.
- 112 Such as CT, PET, SPECT, MRI, DX, and QUS. Computed Tomography (CT), Positron Emission Tomography (PET), Single Photon Emission Computed Tomography (SPECT), Magnetic Resonance Imaging (MRI), Digital X-ray (DX), and Quantitative Ultrasound (QUS).
- 113 Picture Archiving and Communication System (PACS).
- 114 93/42/EC, section 10
- 115 MDR, 21 CFR 803
- 116 The Swedish Data Protection Board has issued an exemption allowing fulfillment of the OFAC-demand for certain companies only (members of the Swedish Bankers Association) and for certain categories of data only.
- 117 E.g., NOMX offer a service supplying material to companies' boards of directors. NOMX run this service from servers in Europe. Running them from the U.S.A. could have increased efficiency.
- 118 Programmes in place to expose misconduct and alleged dishonest or illegal activity occurring in an organisation.
- 119 Directive 2002/58 on Privacy and Electronic Communications (amended by Directive 2006/24/EC and Directive 2009/136/EC)
- 120 Notably, they can access and sell customers' data. Telecom operators are not allowed to view customers' data (only transfer it).
- 121 Consent is not needed for data retention (storage of data) or in cases of suspected crimes. Processing data as part of the actual delivery of a service is also allowed without consent.
- 122 Tele2 supply the SIM card and some services to the vehicle manufacturer. The manufacturer is the data controller, not Tele2 (data processor).
- 123 E.g., insurance companies wanting to use the system to investigate and prevent future accidents (especially non-EU based insurance companies) as well as companies working with automotive safety systems.
- 124 See chapter 4.3.3.
- 125 A solution would be to decide on a business card exception that would remove personal information relating to a work position from the ambit of what constitutes personal information. Like exceptions exist in at least Canada, Mexico, and Singapore. A solution would be to decide on a business card exception that would remove personal information relating to a work position from the ambit of what constitutes personal information. Like exceptions exist in at least Canada, Mexico, and Singapore.



Kommerskollegium
National Board of Trade

Box 6803, S-113 86 Stockholm, Sweden
Phone +46 8 690 48 00 Fax +46 8 30 67 59
E-mail registrator@kommers.se www.kommers.se