A. Industry Feedback on Data Protection and Security Challenges

I. Interview Set-up

A wide range of cloud related professionals (both legal and technical) in California have been interviewed regarding their experience with data protection and in particular the effects of the EU law on their business operations and the industry in general. Hereinafter, the results of these interviews will be analyzed and key issues addressed with a special focus on the new EU General Data Protection Regulation (GDPR).

As the challenges differ for various actors, the unique data protection problems start-up enterprises face are highlighted at the beginning. Subsequently, larger B2B contracting which makes up a substantial part of the cloud market share is addressed. Lastly, a focus is placed on the B2C side with offerings directed at EU consumers. Based on this analysis key points are identified which warrant further research.

The conducted interviews address the general perception of data protection in the context of cloud offerings, such as the weight attached to data protection and security, measures taken to mitigate risk, awareness of the EU data protection law and customer demand. As litigation and class actions are an important topic in US law, these factors have also been briefly discussed in the context of risk shifting in contract negotiations.

Generally, US-based cloud enterprises comprising many SaaS (Software as a Service) solution providers are aware of the high standards the EU data protection law sets. A majority of providers have opted to implement contractual tools, such as the EU standard contractual clauses into their frameworks. These often larger providers have a certain degree of sophistication and thus are able implement measures to satisfy their ongoing compliance obligations. Furthermore, data protection is also viewed more as a data...
security issue that requires the implementation of security mechanisms, including technical and procedural safeguards. All interviewed providers had security measures in place that varied according to the nature of their data. Nevertheless, they all are aware of the risks that data security breaches can cause.

As the main offering of a SaaS provider is its software, this introduces many unknown risks relating to compatibility, updates and other security aspects that may materialize at a later point. These risks are a major concern for all of these providers, which they try to mitigate as much as possible. However, a 100% failsafe software is an illusion. Rather, an approach is chosen by start-ups in which a service is launched and then adjusted once the customer has conducted an initial assessment of its functionality and risks. In this context, the underlying infrastructure has so far been exclusively provided by Amazon Web Services (AWS) as the market leader in cloud IaaS through one of its many server centers around the world. This ensures that the underlying technical measures to maintain security of the service are up to the highest standard, including all necessary certifications that are required for these server centers.

Thus, the risks of the software are based in its programming and provisioning. All cloud businesses that offer a B2B service have highlighted that the data they process is so sensitive that they elect to only process it in a private cloud. Where the data is less sensitive, they would be more willing to use a hybrid cloud but would seek additional assurances and technical safeguards. As hacking of virtual processes has proven to be possible, the hybrid cloud option does not seem to be a sensible choice without further technological safeguards.

II. Cloud Trends and Challenges

Cloud-based systems have undergone a strong development since the early 2000s. Many cloud providers have emerged that provide the basic Infrastructure as a Service (IaaS) on which numerous cloud service providers have built their business operation. This IaaS market is dominated by Amazon Web Service, Microsoft Azure, and Rackspace. They each provide a service for a particular cloud business. For example, Rackspace is viewed
A. Industry Feedback on Data Protection and Security Challenges

as the cloud provider of choice for certain processing operations that require sophisticated hardware, whereas AWS and Azure offer a more standardized and easy to implement cloud environment.

As companies seek efficiency gains through technology, they also want to reduce their operating costs. In order to achieve this goal, flexibility in the service provisioning is required as the cloud is a highly complex construct that incorporates a highly volatile price structure that needs to be adjusted to customer demand.

1. Introduction to Cloud Services

The cloud industry landscape is highly diverse. It consists of Infrastructure as a Service (IaaS) providers, which provide the hardware resources for other cloud services, and Software as a Service (SaaS) providers that offer their innovative software solutions running on an IaaS cloud. Additionally, constantly new forms of cloud services are being developed. Some of these act as intermediary tools which provide a platform based on a IaaS cloud for enterprises that do not have the knowledge or do not want to expend the resources required to implement a complete environment for the software in order for it to run on a IaaS. Thus, these Platform as a Service (PaaS) providers bridge this gap by offering a basic software platform on which the SaaS provider can simply install its service without having to be concerned with managing the underlying IaaS cloud.

2. Costs in the Cloud

Over the last years, the trend in the cloud market has shifted to more integrated services that offer a full range of tools extending to all aspects of a business operation. Furthermore, server centers of the main cloud IaaS providers are now established in every region, including special offerings for the EU. Previously existing price differences between regional offerings no longer play a significant role today, since most large IaaS customers use cloud enterprise agreements that calculate costs based on the use of a service regardless of location of the service provided.161

---

161 Interview 3.
For smaller customers, the regional offerings are, however, still more expensive, as the cost to maintain a server center in the EU is higher. The price difference between North Virginia and Ireland is around 5-10% for small amounts of usage.\textsuperscript{162} If the data is being processed on the US West Coast, then the price is even higher than in Ireland. This just exemplifies how close the pricing has become and the options that a customer has when deciding where the data should be processed. In particular, when the service provisioning does not depend on the fastest possible availability, then a location that is cheapest for providing the service can be chosen.

3. \textit{Latency in the Cloud}

Latency times are, of course, also a factor in this equation. Latency is the time that is required for the data to be processed and returned to the sender. The ease of shifting data within the cloud across regions enables SaaS providers to improve user experience by storing the data in the region the user is currently in and, thus, enabling faster access to the data. This process is called “sharding”.

However, in doing so, this data may become subject to the EU data protection law and require authorization for transferring it outside the EU again once the individual customer returns to his or her home country outside the EU.\textsuperscript{163}

Furthermore, latency is integral to new services, such as autonomous driving and other tools that require real-time communication in order to function properly. In these cases, the servers must be located in the region in which the service is offered. Otherwise the latency times would be too long. Thus, data protection laws restricting such a free flow of data across borders will impose significant obstacles to new technologies, such as autonomous devices, Big Data and the Internet of Things.

\textsuperscript{162} See Amazon Inc. Amazon.

\textsuperscript{163} The General Data Protection refers to persons in the EU thus applying the law also to non-residence that are within the territory of the EU.
4. Identifying Personal Data

Some cloud vendors face the problem of identifying personal data and the location of that data at a given point in time. Essentially, these enterprises only rely on the login credentials of their customers to determine who the individual user is and thus which law applies. However, IP addresses are not a good predictor of location, since they can be altered through the use of VPN tunnels that are becoming more and more mainstream in order to gain access to media content that otherwise would be blocked from access in a certain region.\textsuperscript{164} In particular for smaller SaaS providers, these identification requirements are hard to achieve because they come at great costs.

However, new technologies are currently being implemented using artificial intelligence in order to determine whether data that is being transmitted through a router meets the definition of identifiability contained in the GDPR. If the data does allow the identification of an individual, then the technology automatically replaces the identifying factor from the data before it enters the server. The replacement variable is then stored separately from the data in a secure server to which the processor of the data does not have access. Although this provides a complete protection from the EU data protection law, it remains to be seen whether the data is still of value and whether the re-identification is still possible after conducting processing operations on the data.

5. Security Risks

Cloud security has grown to be a central topic in determining the future of this technology. The risk mainly lies in the hijacking of a user account as it allows a party access to nearly all systems. Two factor authentication is now the common norm in the cloud environment as it ensures that the person is identified not only by the device he or she is using but also by a unique token (key).\textsuperscript{165}

From a security viewpoint, most cloud service providers are taking many measures in order to ensure the integrity and resilience of their systems.

\textsuperscript{164} Interview 2.
\textsuperscript{165} Interview 11.
Already the large IaaS providers supply the tools and technology to ensure a very high level of protection, as they and their customers monitor access in order to identify DoS attacks and other treats to their cloud environment. Furthermore, sophisticated software monitors and limits the actions of the cloud customer to ensure that they do not affect the core function of the infrastructure in any way.

III. Unique Challenges of Start-Ups

Start-ups naturally face many challenges during their first years. These include financial, organizational as well as regulatory factors that constantly pose a threat to the future of the enterprise and must be addressed accordingly.

1. Key Challenge for Start-Ups

Currently, there is a strong trend in the US business sector to engage cloud (start-up) ventures that offer a wide range of ancillary business services in the cloud. These services range from entertainment platforms and scheduling tools to sophisticated document review systems. However, many of these enterprises lack resources (financial and human), and this is why they are required to focus their efforts on specific tasks that can be achieved with the resources at hand and that are vital to the further sustainability of the enterprise.

Based on these constraints, data protection is not a predominant issue although it is factored into the general security of the service offering. A first concern is having a minimal viable service that can be sold to customers and generates revenue to sustain further growth and attract investment. Additionally, any growth will require the retention of skilled labor. As long as the start-up is not processing any special data that is governed by specific laws such as financial or health data, any data protection and privacy measures will not be on the priorities list.

Most ventures use Amazon Web Services or Microsoft Azure as their basic cloud platform for the supply of their cloud services. In doing so, a minimum standard of data security is already created, as these providers have
implemented sophisticated systems to ensure the security and integrity of their server centers that directly benefit their customers. These services allow young enterprises to primarily focus on the development of their software and the acquisition of customers.

However, as the interviews with start-ups and consulting firm members have demonstrated, some enterprises, in particular business enterprises, seek to ensure that the service provided meets certain criteria. Most of these criteria can already be satisfied through the IaaS vendors. However, in some cases, further safeguards are required. These can either take the form of contractual or technical safeguards that then act as a driver for better data protection.

2. **Entering the EU Market**

Once a US-based SaaS start-up decides to enter the EU market, data segregation becomes an important factor in order to keep EU and other data separate for compliance purposes. For cloud start-ups, the environment provided by a large corporation such as AWS is essential because it provides a secure base infrastructure on which the start-up can develop its offering and potentially scale its business with limited costs.166

Selecting the appropriate cloud provider does not seem to be a major challenge, as Amazon dominates the market followed by Microsoft. Rackspace appears to be the provider of choice when it comes to private cloud arrangements.167 With regard to privacy, their services offering and systems are substantially similar. Furthermore, they all use an enterprise agreement which charges the customer based on usage. In particular, AWS and Microsoft have regional (generally 4-5; e.g. US/EU/Asia) offerings. Thus, data transfers can be restricted to the data centers in one of these regions.

---

166 Interview 2.
167 Interview 5.
IV. Processing of Sector-Specific Health Data

Health data is a very special category of data that is subject to many protection regulations. Firstly, it is protected as personal data by data protection law as such and the GDPR that imposes a higher standard on it as sensitive data. Additionally, health care laws limit the ability to process such data according to EU Member States’ law, as well as HIPAA. Furthermore, often credit card or financial information is stolen in the context of a security breach, and any potential damage that may result is unknown. This is why courts are reluctant to grant any form of compensation going beyond a credit monitoring service where there has been no immediate damage to the affected individual’s credit history or fraud.

Thus, the first step for any cloud professional is to understand how the pre-existing laws may apply to the cloud business model. This includes a target approach to the required level of security, which often differs between compliance professional and information technology security experts.

Various laws affect cloud and other service providers’ obligations to implement security measures. However, most of these laws relate to specific types of data such as financial or health data and are governed by separate laws. In the financial sector, the Gramm-Leach-Bliley Act (GLBA) is one of the most important financial regulations covering also the topic of information privacy. This includes an obligation to oversee service providers that regularly include cloud providers. Thus, when selecting a cloud or other service provider, the financial market enterprise must ensure that the provider can demonstrate appropriate safeguards, including contractual rights and duties. However, only reasonable steps must be taken to ensure service provider security. What is reasonable will largely depend on the given circumstances. Nevertheless, clarification taking into account the ability to monitor or influence the cloud provider should be

168 Such as financial market regulation, consumer protection, data protection and communication law.

169 FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.4(d)(1).
A. Industry Feedback on Data Protection and Security Challenges

provided in order to realize the needed market certainty for the wider use of such technology.

Similar risks exist in the content of health data being processed or stored in the cloud. US-based enterprises must comply with the Health Insurance Portability and Accountability Act and its subsequent modification by the Health Information Technology for Economic and Clinical Health (HITECH) Act. These laws, similarly to the financial regulation, require enterprises to take steps in order to meet the requirements of the law. In this context, again the reasonableness of the measures and their appropriateness to protect the health information will be assessed in case of an audit. However, they also include some specific measures, such as regular risk analysis, the assigning of unique user names, as well as the action taken in response to incidents or threats. Of particular importance is the fact that the enterprises transferring data into the cloud will remain liable for non-compliance of their service provider.

Compliance with HIPAA is very costly, which is why Microsoft and other cloud providers include specific services and contracts for the provisioning of compliant cloud services. For example, Microsoft HealthVault requires the signing of a business associate agreement aiming at ensuring that the data will only be used or disclosed in accordance with HIPAA. In any case, known breaches must be addressed immediately no matter whether the conduct of a subcontractor or a company’s own doing gave rise to the event. When contracting with the federal government, rights to access and inspect the premises must be granted. Whether this applies to a subcontractor’s subcontractor (e.g. in a multilayered cloud) is unclear.

In light of the already existing complexity of various new technologies, these laws should be amended to ensure clearer rules are used which enable service providers to understand what their obligations are and how they can be met. However, as this process is very slow and inflexible, the

---

170 Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191, 110 Stat. 1936; Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 17931-40 (2011).

171 Ibid, 45 C.F.R. § 164.308-312.
innovative industries have started to implement their own codes of conduct that act as a self-regulatory mechanism, which aims at ensuring that the government cannot interpret a certain statute differently when all of the industry applies it to a new technology in a certain manner.\(^\text{172}\)

Informing customers and the persons whose data is being processed of their rights and obligations after the contract is terminated is also central in order to providing the transparency that legislators seek to achieve. With this information, service providers could also better assess their compliance situation and design a path to achieving the goals of the law.

**B. Business to Business in the Cloud**

**I. Current Developments**

**1. New Technology**

Cloud applications are extensively used in the Business to Business (B2B) context. A vast amount of new services providers have emerged over the last five years, which aim at improving the efficiency of business operations. Generally, the contracting parties in this scenario have a high expertise with regard to the cloud offering and its requirements. They are able to understand the international data flows through the cloud services and the possibilities available to mitigate risks that both affect legal compliance as well as the security and integrity of the system.\(^\text{173}\)

In the B2B context, the SaaS provider will often reach an agreement with the IaaS provider containing a clause allowing it to shift the data between server centers of a particular region. This includes a decoupling of the infrastructure and a mapping across all contractually agreed jurisdictions.\(^\text{174}\)

\(^{172}\) For example the credit card industry has published its own guidance on data security in the context of cloud computing see <https://www.pcisecuritystandards.org/document_library>.

\(^{173}\) See Part I, B for a detailed overview of the available cloud services.

\(^{174}\) Interview 3.
Furthermore, most enterprises elect to use a private cloud offering as the hybrid alternatives still carry a significant risk. The tools offered through hybrid clouds are highly effective, for example, in order to manage a project. However, the risk lies in the combination of these tools with other software, such as an internal communication tool (e.g. Slack) that increases the risk of unwanted disclosure of personal or confidential data. These tools can be used to breach an otherwise secure system.\footnote{Interview 6.}

Although all actors in the SaaS context wish to ensure security, the dichotomy of ease of access and security is still hard to bridge. Thus, innovative tools often cannot be recommended based on their perceived risk to the existing infrastructure and the business operation.

2. **Contractual Innovation**

Managing the level of trust between sub-processors is a key topic in dealing with various cloud vendors. This includes regular audits of the business partners’ operations and a contractual requirement that they do the same with their respective vendors.\footnote{Interview 4.}

One of the trends in relation to data protection has been the use of more explicit data security terms in contracts. These include detailed descriptions of security requirements in the form of lists, as well as classifications and definitions of data breach scenarios. Such clear terms are necessary as the nature of data breaches can be highly complex and involve a number of actors. In contrast to the EU, the US system of risk allocation relies more on commercial practice than on law.

However, although many customers seek to get a carve out for data security breaches, smaller SaaS providers are not willing or able to take on this risk. Thus, innovative approaches are used to get around the limited liability for data security breaches. These approaches try to introduce essentially the same liability as for data security breaches by claiming a breach
of confidence based on the disclosure of confidential information to an unknown third party.\textsuperscript{177} In most cases, the breach of confidence provisions do not contain a liability cap that allows for the introduction of unlimited data breach liability through this back door. The only way to counter this situation is to have a large Annex, which sets out the requirements in order to trigger either the data breach or confidentiality provision. Once these have been set out, the parties can then agree on a liability cap.

3. \textit{Challenges for Cloud Vendors}

Cloud vendors as well as business customers regularly require outside specialists who can ensure that their infrastructure and software is secure against any external and internal threats. Some of the most important security trends over the last decade include a growing use of encryption as well as the “sharding” of data across jurisdictions in order to limit the risks of potential data loss. Furthermore, government access and the ability to track individuals (so called shadows) across the Internet have changed significantly.\textsuperscript{178}

Since Edward Snowden’s revelations, enterprises in the online world are increasing their data protection through encryption as well as pushing back on data request by government agencies. On the user side, technologies such as Virtual Private Networks (VPN) with cascading functions allow a user to obscure his or her location and encrypt any communication. All these measures have resulted in overall higher protection of data on the Internet than what has been the case in the last 10 years. The awareness of the risks of communicating data in an unencrypted fashion has risen leading to a higher demand for secure services in all areas of online service.

4. \textit{Business Consultation Trends}

Most of the IT consulting work is done in the B2B context rather than the B2C business. In particular, specific compliance obligations under health

\textsuperscript{177} Interview 6.
\textsuperscript{178} Interview 10.
B. Business to Business in the Cloud

care and financial services law affect smaller companies. This is where the cloud can provide the highest benefit. Cloud-based start-ups now address the varying environment and security aspects that must be in line with the legal requirements. For example, a mobile device, a cloud server and a laptop operate in differing environments.

Vault is a software that provides one environment for all these platforms and allows for secure testing and easier compliance with HIPAA and other laws.

5. Transatlantic Cloud Data Centers

Data centers are subject to three main considerations, including costs of running the center, latency times as well as local laws. In the EU, cloud providers often opt for Amsterdam as one of the server locations as its laws favor cloud computing and its connection speeds are ideal. This also applies to Switzerland with its good communication infrastructure. However, costs are higher in Switzerland than in most EU countries. Furthermore, by processing data only in the EU, the redundancy as well as the availability would be limited and increased latency is also expected when the data is accessed outside the EU. Most US-based vendors now opt to categorize their data into non-EU and EU data as currently the EU data protection law carries the most restrictions.

Data center providers have even gone so far as to test underwater data centers that would require less power because the seawater takes over much of the cooling. These centers can theoretically be placed near any coastline, thus raising jurisdictional questions. Based on these technological developments, the data protection laws are slowly expanding their extraterritorial reach, starting with the GDPR which subject any enterprise that offers good or services to natural persons in the EU to its high data protection standard.

II. Ancillary Business Services

Most US-based companies have adopted a strategy of focusing on their core business and obtaining all ancillary tools and services from third
Ancillary Business Services

party vendors. This enables them to focus on their own product or service. Often other providers will already be able to supply a software module, which would otherwise cost a fortune to develop. An example of this is a translation tool required for many SaaS applications.\(^{179}\)

1. **SaaS Human Resource Tools**

Managing a company’s human resource has become more demanding as the expectations of employees have grown. In order to ensure a high employee retention rate, companies must use the most up-to-date human resource software. This includes human resource cloud tools such as the Cornerstone offering, which enables all steps from selecting a candidate, onboarding as well as compensation management to be carried out in the cloud. With these systems, a considerable amount of personal data is being processed, including financial, racial as well as other sensitive information.

As most customers of such systems are large multinational corporations that depend on such tools to manage their international workforce efficiently, cross-border transfers of data are often a necessity. For example, when an EU subsidiary of a multinational corporation manages its employee data in the cloud, this information will invariably be transferred to the US-based cloud provider at some point. Mostly, these transfers are carried out under the standard contractual clauses exception to the DPD, since they are easily implemented and are well known to the vendor as well as the sophisticated business clients.

In the ordinary course of business, the cloud service provider will offer its clients alternative locations for the data processing. These locations closely mirror the current data protection laws around the world and are divided into US, EU and other country offerings. Regularly a combination of EU-based processing, together with a country that is considered as providing adequate protection under EU data protection law, is used in order to offer ancillary services. For example, customer support hotlines as ancillary services can be located in countries such as Israel (a country considered to have an adequate data protection standard), which are closer to the local

\(^{179}\) Interview 8.
customer time zone. The selection of the EU as processing operation is mostly viewed as a political and sales issue as there is no technical difference whether the data is being processed on the US or EU cloud. The cloud service provider is bound by the same contractual obligations as when it is processing the data in the EU.180

However, due to US surveillance laws that allow for access to US-based data and the geographical limitation of the Stored Communications Act (SCA)181 to the US, great differences with regard to public access rights in the EU remain. These limitations are based on the outdated nature of the SCA, which still works on the assumption of point-to-point data transfers and an arbitrary distinction between the duration for which the communication is stored.

Thus, when data is stored in the EU, it is generally safer from access by US public agencies that seek to access the data under a US court order. Most large SaaS providers have evaluated the risk of disclosure under, for instance, the Patriot Act and have determined the risk to be fairly low.182

Currently, these providers closely monitor the situation in the EU with the GDPR, the Privacy Shield Agreement, as well as the Brexit. In any case, they ensure to their EU customers that they are prepared to take all necessary steps in order to comply with EU data protection law even if this means shifting data from UK data centers to an EU country.

As the data used in the HR context contains also sensitive personal data, the cloud service providers interviewed have opted for their own dedicated servers (separate from other servers), which are provided by a third party contractor such as AWS. The SaaS provider also contractually ensures that the Iaas provider maintains certain security certifications, such

180 Interview 1.
181 Stored Communications Act Pub.L. 99–508.
182 Interview 1.
as the ISO 27 000 certifications\textsuperscript{183} as well as Social Security Administration, and other relevant US and EU certifications. Furthermore, not even the coders have access to the data being processed, since this is not required to improve system functionality. Data access is closely logged and only available to a select number of employees. In any case, these providers treat all data as personal data in order to avoid any shortcomings.\textsuperscript{184}

The continuous and regular evaluation of data protection risks has become commonplace in most SaaS settings. Often, a data protection group is established that comprises of employees from IT, legal and management who meet up on a regular basis to discuss any potential threats relating to data protection, privacy, and security. Furthermore, before a new feature is implemented, the IT and management team assesses its risks with regard to these factors.\textsuperscript{185}

2. \textit{SaaS Application Monitoring}

An infinite number of applications enable businesses to communicate, appraise, market and control their operations. These tools all run in the cloud and have the potential to malfunction at any given point for a vast array of reasons. Thus, in order to identify issues as fast as possible, SaaS application monitoring is an essential element in reducing risk and resolving any system glitch that may arise. AppDynamics is one of the most successful cloud providers offering such a service to many different service industries, including banking, insurance, retail, and wholesale. Two forms of solutions are provided for customers wishing on premises or off-premises hosting in the AWS cloud.

\textsuperscript{183} ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.

\textsuperscript{184} Interview 1.

\textsuperscript{185} Interview 1.
The monitoring system utilizes so-called agents that accompany a process, e.g. a java engine, and report information on that process to a central control element. If a customer selects to have these agents for all of its processes, the application provider is able to monitor the performance of the entire infrastructure end-to-end. As this service is not concerned with the content of the process, the provider does not gain access to it. This is an important factor in the design of the system in order to focus on the service without the risks that come with unnecessary access. Providers even go so far as to contractually oblige their customer not to design an application in a manner that would allow them to gain access to the data. The most personal data that the provider receives is an IP address of a user from which certain information may be derived, such as the location of the computer.

In addition to the main process monitoring tool, another service that directly analyses log files may also process personal data. This tool mines log files for analytic purposes in order to identify issues that may have arisen in the use of a service. These logs can contain a wide range of data depending on how the customer has designed their software. Thus, in order to limit risk the customer is contractually prohibited from storing personal data or other sensitive data in these files. Furthermore, if such data is included, the customer will bear all risks associated with the vendor’s software mining this data. From a vendor’s perspective, their engineers ensure that they only access the performance data and no other information.

The EU subsidiary is required to conduct privacy protection audits according to a strict list of procedures which are in line with the EU data protection law and the company’s own internal standard. When the cloud provider itself contracts services from third parties, a detailed “playbook” also regulates this process, including the decision-making process as well as what and from whom data is collected. Often this includes the discussion of whether the contracted party is a controller or processor for purposes of EU data protection law. When the ultimate determination of the party’s nature is unclear, companies often opt for the processor classification as it
Ancillary Business Services

carries a lot less obligations than a controller.186 However, with the GDPR the obligations of the processor will also be increased.187

3. Customer Success in the Cloud

Ensuring the satisfaction of all customers is a key factor to a successful business. In order to achieve this goal in the online world, an in-depth understanding of the needs and issues of customers is necessary, which requires the collection and processing of a vast amount of data. Previously customer services were reactionary, meaning that the company only addressed an issue once it had been raised by a customer. Today, the service provider seeks to be more proactive in meeting the needs of its customers by offering flexible solutions.

In order to increase customer satisfaction and providing a tailored service, sophisticated data analysis is necessary. This includes data from various data silos, including Salesforce, billing records, communication protocols and log files. Cloud service providers are able to copy this data into the cloud and predict which customer requires what sort of attentions. For example, customer retention rates can be increased, as well as tailored service solutions offered, based on the need of the customer. Furthermore, dynamic pricing can be integrated in order to increase revenue by up-selling or cross-selling products and services.

The use of these innovative technologies is hindered by EU data protection law, which sets strict requirements to the processing of personal data and its transfer to a US cloud. Thus, a potential solution would be the pseudonymization of the data under which the processing is carried out. Once a course of action or conclusion has been drawn, the customer then re-identifies the person to whom the data applies.

However, the compliance requirements of the GDPR weigh heavily on any innovative form of Big Data analytics, as it carries the potential to identify an individual even with anonymized data because of the vast amount of data that can be merged and analyzed to determine previously unknown

186 Interview 7.
187 General Data Protection Regulation, Articles 12 et seq.
patterns. Based on these patterns, the re-identification of an individual becomes possible.

For example, an IoT device collects information on the behavioral patterns of an individual. This data could be processed very freely in the US as long as the customer has consented by, for instance, buying the device or accepting the terms of service contained in the app he or she downloaded to monitor or manage the IoT device. In the EU, this data will likely be viewed as personal data based on its potential to indirectly identify an individual. However, currently the technology and its legal environment are still at an early stage. Providers of such services can thus only seek to inform the customer as detailed as possible of the risks involved in the collection and processing of the IoT data and its potential to infringe privacy.\footnote{Article 29 Data Protection Working Party.} Securing access to the data and in particular the aggregated data from various devices is a key obligations of such data controllers. This must be taken seriously, since a data breach can have severe effects not only on the individual but also the integrity and security of the backbone of the Internet.\footnote{This has been demonstrated by the hacking of the camera software of DAHUA Technology and its subsequent use as a botnet aimed at bringing down the Tier 1 Internet service provider Level 3.}

In particular, the consent and notice requirements contained in Article 5(3) Directive 2002/58/EC must be adhered to, which require effective consent after obtaining clear and comprehensive information about the purpose of the processing.

4. \textit{SaaS Legal Services and Discovery}

Over the last years, new service providers have emerged that offer innovative SaaS that allows the managing and storage of legal documents in the cloud and the hiring of specialized attorneys on a project basis. Furthermore, new electronic discovery tools are being offered in the cloud.
4.1 SaaS Attorney Tools

In international corporations increasingly new SaaS tools are used to increase efficiency of legal processes. These systems often process a wide range of data, which includes all data surrounding the efficient billing and management of the system and the data that is uploaded by the customer. However, this necessarily includes information on the parties as well as the nature of the document. With this information, statistics can be generated for the customer to show what sort of legal services are most commonly contracted out or what the average price of a certain task was.

In order to provide a complete service to the customer, a certain degree of analytics is carried out on the metadata of the documents provide as part of the service. This enables the SaaS provider to compile a list of how many referrals for a particular transaction type came from which business partner. Furthermore, average turnaround time of documents as well as escrow percentages are ascertained in order to enable the improvement of the customer’s business operation.

At no time does the company want or seek access to the documents that are being exchanged, since this is not required for the provisioning of the service and would only increase the risks of the business by enticing employees to monetize this information.

Based on the requirements related to security, such SaaS offerings often run on a secure and reliable AWS cloud. With regard to data protection, security issues and a potential data breach are the main concerns for an enterprise, as the information that is being communicated through the software is the most valuable data a company has. For example, this includes pending negotiations, intellectual property and other commercially valuable information. In order to address these risks, many providers use a two-layer authentication in order to ensure that the person logging in is
correctly identified.\textsuperscript{190} Most of the risks exist at the user end, thus it is essential that all hard drives are encrypted and that the attorneys who are not familiar with the newest technology are appropriately trained.

In order to address some of the issues the market has started to respond.

(1) The developments in the last years show that the awareness in the market of data breach issues has grown and more questions are being asked in this regard.\textsuperscript{191} However, there is a certain limit as to what resources can be expanded to protect data. Most providers do their best to ensure the safest possible environment for their SaaS applications. Nevertheless, a risk still remains, which is why encrypting data not being processed is an essential measure for any SaaS provider.

(2) Exclusion clauses are being used to limit liability outside the control of the vendor’s powers. Currently, most SaaS start-ups only have a general insurance that covers a basic amount for data breaches. However, as these smaller SaaS start-ups are growing, they are also looking to increase their insurance coverage, including potentially buying specific insurances for data breaches.

But some risks may arise when data that is subject to special laws is being transferred across the provider’s systems. For example, HIPAA data could be part of a wrongful employment termination claim and thus included in the documents exchanged over the SaaS platform, ultimately making the provider subject to this law. The issue is that in this case the provider will not know of the HIPAA data and thus not be able to ensure compliance with any applicable provisions of the law.

The EU market currently does not seem to be of interest for SaaS in the legal field based on the vast amount of varying jurisdictions and laws. Only in ancillary cases, for example the sale of an EU-based company to a US company using the SaaS platform, challenges with regard to EU data

\textsuperscript{190} Two-layer authentication requires the user to be identified by his or her device as well as password. Thus, a second layer of security is added by sending a temporary identifier to the device e.g. mobile phone.

\textsuperscript{191} Interview 5.
protection law may arise. In this situation, data must be transferred to the US for due diligence assessments, which are carried out by US-based attorneys and accountants.\(^{192}\)

### 4.2 Discovery in the Cloud

Discovery in civil law cases is a fundamental concept of US law. Before a trial, the defendant is obliged to hand over all relevant information pertaining to the claim made. This can entail a wide array of data including electronic records. Often, enterprises store and process data all around the globe and are not entirely aware of what data is relevant for a case. Thus, in order to avoid the impossibility of searching millions of records, sophisticated software with machine learning capabilities is available that can enable a fast shifting through such data in order to determine what is relevant for the case at hand. However, the court will usually be required to approve a particular system, as there is often a disagreement as to what software and search technology to use. In order to level the playing field for all claimants and defendants, judges must be appropriately trained and keep up to date with technological developments.\(^{193}\)

The discovery process within an international enterprise can be highly complex based on the different jurisdictions in which data is stored. For example, when a Chinese company has a subsidiary in the US and in Sweden, the issue can arise that the parties may want to ensure that no data is being transferred to China during the discovery process due to security and confidentiality concerns. In these situations, innovative compromises have to be reached. When EU data is involved, often waivers are obtained from the employees in order to transfer the data to the US and present it to the counterparty.

In the context of third party disclosures, companies will often seek indemnities from the court before making a disclosure. However, the argument that a third country’s local laws would be violated if data is disclosed will often not be sufficient to avoid disclosure. The New York Appellate

\(^{192}\) Interview 5.

\(^{193}\) Staiger, Die Zukunft des Datenschutzes in einer globalisierten Welt, 147 et seq.
Court\textsuperscript{194} decision may have slightly shifted this position. Nevertheless, as in the civil discovery process where mainly monetary disputes are resolved, the courts are not bound by the strict rules of criminal procedure.

A practical example of the boundaries of electronic discovery is the data that is being collected in pharmaceutical studies. In these situations, a court order is essential in order to protect the confidentiality of the information.

Vendors of cloud-based electronic discovery services such as Everlaw\textsuperscript{195} or Logikcull\textsuperscript{196} are closely vetted by law firms, which includes on-site checks during which the security and infrastructure are inspected. Sometimes this also includes penetration testing carried out by an independent third party. Based on the international nature of today’s electronic discovery, a cloud solution presents a perfect solution to carrying out international discovery without the need to train the system for each country.

In order to process the data, the cloud provider must first prepare the information for its system. However, soon this step will be carried out automatically, allowing the customer to upload any data into the cloud for discovery. Additionally, in order to meet the demand in other counties such as Australia, local AWS instances in the cloud are utilized. Maintaining an Australian domain requires a registered business, which then raises the need for a registration of a trademark in order to protect the company’s name.

Running on cloud process for a global operation is currently impossible, since national data protection laws in various jurisdictions hinder the data transfer. This leads to potentially different search patterns for the same case being run in a number of countries. Ultimately, this disjointed processing compromises the integrity of the systems although the result may be the same.

Essentially, the machine learning process must be carried out repeatedly which leads to unnecessary costs and time consumption. Furthermore, if

\textsuperscript{194} In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp. v. United States Docket No. 14-2985.
\textsuperscript{195} <www.everlaw.com>.
\textsuperscript{196} <http://logikcull.com/>.
data of a company subject to the discovery process is mingled across instances, the accuracy increases. This is in the interest of the court process and in the interest of the defendant to avoid unnecessary disclosure. Often consent is sought to address this issue.

However, the amount and types of data are so vast that they may touch upon third party rights and thus the consent sought may not be adequate. When there is a risk that copyright or intellectual data is involved, systems are used that only allow the display of the result of the processing in the foreign jurisdiction, as in these cases no persistent storage is created and no potential copyright infringement occurs. The GDPR litigation exception also provides for a further mechanism under which the personal data can be processed in the context of a litigation.

Access to the data is only possible through two-way identification, using tokens which ensure that the party gaining access has identified itself through the device as well as his or her unique key. On the cloud processing level, hardware resources are shared by other instances. The discovery process, however, is protected by an encryption layer that prevents access by other instances.

In addition to the processing of data for discovery purposes, electronic discovery providers are interested in collecting aggregated anonymous data in order to improve service accuracy and user experience.

4.3 Trends Identified by Law Firms

Major law firms dealing with international corporations are seeing a higher use of escape clauses in contracts, which allow parties to get out of M&A deals or other transactions. Furthermore, the amount of employee records used in employment-related litigation has increased in particular with reference to compensation and performance and its comparison to others.

---

197 Interview 8.
198 General Data Protection Regulation, Article 12.
199 Interview 6.
B. Business to Business in the Cloud

If a necessity for a data center in the EU exists, Switzerland is seen as one of the top choices as it enables corporations to move data in and out of the country easily. However, the higher costs in Switzerland are a certain drawback. In relation to Germany, some hesitation exists to move data centers there, as the German framework is viewed as being too strict. With the potential effects of the UK leaving the EU, US-based enterprises are seeking an alternative for UK-based data centers.\(^{200}\)

Law firms are required to use one of the main office products in order to draw up their legal documents. The most commonly used software is Office 365. The cloud solution can be adjusted to the data being processed, thus even a HIPAA-compliant offering is made available by Microsoft. However, using software remotely still is not an option for law firms as this would include the automatic pushing of updates, which could compromise the integrity of their systems.\(^{201}\)

5. **SaaS Communication Tools**

Many new communication tools that are cloud based have been introduced to the market over the last couple of years. Essentially, they all provide a basic functionality, which is the communication of employees within their corporate structure as well as a tool for outside customer communication. Additional features include a linking of these tools to software development tools, as well as a wide range of already established services such a SMS, Web meeting tools and Email. The service is facilitated by transferring the data through the cloud of the CaaS\(^{202}\) provider.

As this service integrates aspects of a cloud offering and communication tools, both data protection laws as well as the laws relating to the protection of communication such as the E-Privacy Directive apply to these providers. In this context, US-based companies often have a UK or Irish subsidiary from which they offer their services to the EU market. As some of the communications are done not only over the internet but also through

\(^{200}\) Interview 1.  
\(^{201}\) Interview 5.  
\(^{202}\) Communication as a Service.
a chat tool, this data must be stored at least for a limited amount of time. Due to EU data protection law, this is often done locally as otherwise issues concerning trans-border transfers of personal data may arise. However, as data may be transferred from the EU to the US, the subsidiary in the UK and the US headquarters will have a contract in place containing the EU model clauses.

A major challenge for communication tools which allow employees from different locations to send each other information is the fact that such a tool may lead to the communication of personal data of customers or other parties, which are then subject to EU data protection laws. In order to achieve compliance in this regard, the employees receive regular training and the functionality across various software programs is limited to the extent possible. Furthermore, the EU party contractually assures that such data will not be communicated through the tool and that it will indemnify the service provider from any claims made. However, the indemnity clause is often not an option based on the lack of negotiating power on the part of the CaaS provider. Currently, boilerplate agreements are biased in favor of the vendors. However, in all cases essential elements such as certification requirements, compliance undertakings, and security terms must be included.

With regard to government access to data, CaaS providers also strongly limit the amount of data they collect unless it is necessary to provide the service. However, as the main focus is on facilitating communication, the amount of data that needs to be collected is limited. Often a first-in-first-out approach is chosen for chat functions, where the oldest data is deleted first once a set limit of storage has been reached. Additionally, sector-specific data will be excluded from the service through the contract. For example, health data cannot be stored or communicated on a provider’s systems without prior approval, as the compliance requirements are high and this would increase the cost of the service.

---

203 Interview 9.
204 Interview 9.
205 Interview 9.
6. **Extension: Public Services in the Cloud**

With the rise of cloud computing and Big Data in the private sector and its widespread adoption, government agencies also seek to benefit from this technology. Often government agencies have their own servers, which are costly to maintain and do not scale easily. The US government has taken steps to shift its data processing to the cloud, whilst addressing its risks through the Federal Risk and Authorization Management Program (FedRAMP). As most of the standard terms in cloud contracts are unacceptable to the government, special procurement methods are adopted. Nevertheless, even if a public procurement procedure is used, knowledge of the risk management measures and requirements that the government must set needs to be retained as otherwise bargaining power will not suffice.

Often only a smaller number of service providers put in their offer for setting up an IT infrastructure for a public entity as the process is very long and tedious. Furthermore, many additional requirements are imposed based on stricter data security requirements, whilst at the same time facilitating the disclosure of data under a freedom of information request. The existing government systems must also be taken into account, which do not undergo the faster replacement cycles as in the private sector.

C. Business to Consumer in the Cloud

The interaction with consumers who use a cloud service carries many obstacles for cloud providers. These are based on the higher protections afforded by various laws, such as consumer protection laws as well as the difficulties inherent in understanding legal communications. Thus, marketing services providers generally only offer a limited standardized service, which is subject to a standard contract that has been vetted against

---

206 In particular since the US government is one of the biggest purchasers of cloud computing services it has the power to influence the terms. See Fed. Chief Information Officers Council, Chief Acquisition Officers Council & Fed. Cloud Compliance Comm., 2 (maintaining that “the Federal Government holds the position as the single largest purchaser in this new market”).
other commonly acceptable terms. Such an approach enables a reduction of potential risks as well as taking into account of the lower margins and transaction volumes of these contracts.

I. Data Protection Implications

From a data protection viewpoint, these service offerings to consumers pose unique challenges. Firstly, the data that is collected from these individuals in some form always contains personal data, requiring the cloud provider to fulfill notice obligations including information on the nature of the processing operation; the rights of the data subject, such as deletion and rectification rights; as well as any particular risk arising from the processing and the use of subcontractors.

Furthermore, the data flowing from an individual is mostly not grouped into specific categories and the nature generally unknown to the service provider. In the commercial context, these factors are individually discussed, thus resulting in a better understanding and tailoring of the ultimate service use. However, this also depends on the nature of the cloud service, as an IaaS provider will generally have less involvement in the processing whereas an SaaS provider will provide software tools which only allow for certain processing operations.

Consent in this context is also a major point because the data collected in the cloud may be combined or used with other data. The user must thus be made aware of such risks to be able to make an informed choice on whether he or she wants this to occur. Ownership rights of the uploaded data is also a key topic in this context. Often, the right to the data is lost when payments are outstanding. Furthermore, the data in the B2C context is not retained very long after contract termination, making it hard for individuals to restore the data. Social media sites also favor storage of the user data even when the contract of use is terminated in order for these sites to improve their service for other members.207

207 Council of Europe, 8.
C. Business to Consumer in the Cloud

Mostly, the information imbalance as to how the service is provided and what the precise nature are of the rights and obligations of the parties under contract limits the ability of the individual to make an informed decision. With the introduction of the GDPR, these requirements as to the consent of an individual are subject to higher scrutiny. ²⁰⁸

II. Consumer Protection

A wide number of consumer protection laws both in the EU and US apply to a B2C scenario. In essence, they aim at ensuring the customer is able to make an informed choice as to the service or goods that he or she buys. Ultimately, unfair competition by, for instance, not giving required notice as to who is operating a website as well as basic contractual terms, would fall under this broad scope.

The FTC takes also a strong stance on these issues by regularly investigating data security and privacy practices of enterprises. It further issues guidelines on specific topics as to what conduct it requires from certain service providers. This approach, for example, includes guidance for mobile health app developers. It sets out that an enterprise should endeavor to collect as little data as possible to limit its burden to ensure security and data protection obligations are met.

De-identification is then the second step. When data is de-identified, it cannot be reasonably associated with a particular individual. A key to effective de-identification is to ensure that the data cannot be reasonably re-identified. For example, U.S. Department of Health and Human Services regulations require entities covered by the Health Insurance Portability and Accountability Act (HIPAA) either to remove specific identifiers, including date of birth and five-digit zip code, from protected health information or to have a privacy and data security expert determine that the risk of re-identification is “very small.”

²⁰⁸ See Staiger, Die Zukunft des Datenschutzes in einer globalisierten Welt, 150 et seq.
Appropriately de-identified data can protect people’s privacy while still allowing for beneficial use. For example, if an app collects geolocation information as part of an effort to map asthma outbreaks in a metropolitan area, the enterprise should consider whether it can provide the same functionality while maintaining and using that information in a de-identified form. The risk of re-identification of location data can be reduced by not collecting highly specific location data about individual users, by limiting the number of locations stored for each user, or by aggregating location data across users.

D. Big Data Analytics Challenges

The study has shown that enterprises are collecting more and more data relating to individuals, which they seek to use in order to improve their existing products as well as to develop new products and services. This is an overall trend around the world but is particularly dominant in the US due to the vast possibilities to use this technology without many restrictions.209

New IoT devices collect more detail-rich data related to human behavior and relationships as well as human biology. Such information creates an immense potential for researches both within enterprises and public institutions. At the same time, the tools for data analytics are also improving, opening new research possibilities. However, this innovation comes at the price of securing the privacy of the individuals whose data is being processed and of protecting their personal liberties. The current regulatory framework is ill-suited to address these issues and any regulation should aim at enabling its use whilst respecting fundamental principles of ethics and privacy.210

209 President’s Council of Advisors on Science and Technology.
210 Vayena, Gasser, Wood, O’Brien, Altman, 423.
I. Research Issues

1. University and Business Cooperation

Often enterprises pair up with universities and other research institutions in order to gain access to the vast pool of resources these institutions provide. In return, they provide the financial backing as well as the data necessary for the research. However, this approach circumvents the oversight that would otherwise be imposed by virtue of a government funded research project. For example, Facebook and Cornell University conducted a behavioral study on Facebook by showing users various types of information and measuring their mood. As the users were not made aware the purpose of this research, the study attracted wide criticism.211

Another example is Netflix, which made some of its usage data public after anonymizing with the aim of improving its service. However, through sophisticated algorithms, individuals could be identified. Furthermore, GlaxoSmithKline has also sought to utilize the iWatch data for arthritis research. This highlights a clear demand for such data, whilst at the same time the risk and compliance requirements are often unclear.212

2. Big Data Research

Research has demonstrated how challenging privacy is in the context of large data sets used in the context of Big Data. These data sets have many data points associated with a given record and thus make the record highly unique and thus identifiable.213 On the one hand, the technology helps daily lives by improving health care, social service, as well as other important connection in our daily lives. On the other hand, these tools also undermine the existing privacy protection laws that are currently in place and are eroded by the vast capabilities that are inherent in large data collection.

211 Accordingly an approval by an institutional review board should have been sought. See Grimmelmann, 219 et seq.
212 Interview 12.
213 De Montjoye, Radelli, Singh, Pentland, 536 et seq.
Often data is collected from an enterprise by a third party research team, which has no means of informing the potentially affected data subjects of the processing operation. Currently, the law mostly regulates the initial stage of the data collection and creation but fails to place a focus on the subsequent use, such as transformation and dissemination. In these cases, data subjects have limited possibilities to revoke, withhold or modify their initial consent.\textsuperscript{214} Thus, technical solutions are necessary, enabling, for example, a dynamic consent.\textsuperscript{215}

In 2014, the disparity between the contractually granted rights to Jawbone, a producer of a fitness tracker, and customer perception was suddenly brought to light in the minds of its customers. During an earthquake, the app registered when a user woke up and the company was able to release this data showing how the wearers of the device were disrupted. Up to this point, many customers were not aware of the vast amount of data these devices communicate to their producers.\textsuperscript{216}

3. \textit{Anonymization and Big Data}

Although anonymization and de-identification are brought up as solutions to the issue of processing IoT data, these technologies do not present solutions as the amount of data is growing at such a rate that even anonymized data can lead to the identification of an individual when combined with a number of other data sets from various sources. This has increased the risk of violating discrimination laws both in the US, Europe, and Switzerland.\textsuperscript{217} Additionally, the perceived privacy risks may slow down the adoption of innovative Big Data processing, which are socially useful or help to increase the overall efficiency of an economy.\textsuperscript{218}

\textsuperscript{214} Vayena, Gasser, Wood, O’Brien, Altman, 431.
\textsuperscript{215} See Kaye, Whitley, Lund, Morrison, Teare, Melham, 143.
\textsuperscript{216} Watson, Ask the Decoder: Did I sign up for a global sleep study?, Al Jazeera America, 29. October 2014, \texttt{<http://america.aljazeera.com/articles/2014/10/29/sleep-study.html>}.\textsuperscript{217} Bolliger, Feraud, Epiney, Hänni, 29.
\textsuperscript{218} European Union Agency for Network and Information Security (ENISA).
privacy concerns, other factors play an important role such as personal autonomy that shapes the Big Data debate.

Technology is a strong driver of Big Data processing. A key enabling technology has been the development of cloud computing and dispersed processing. Thus, when analyzing Big Data and its effects, one must take account of the underlying technology and its risks and advantages. Over the last years, the interoperability between various Hadoop-based\textsuperscript{219} processes has been improved, thus enabling processing across various platforms and higher levels of implementation.\textsuperscript{220}

A core design element of cloud environments is the security of the data environment. In this respect, open source offers some unique benefits, since a vast amount of professionals work on improving the system. This is not the case within a corporation based on a proprietary system, which is subject to resource limitations. Furthermore, one should be aware of the difference between hardware and application compliance. For example, a cloud infrastructure could be HIPAA compliant based on various technical safeguards, but the application running on it may not be HIPAA compliant. Often the requirements as to the application design differ substantially from legislation to legislation (e.g. SOX and HIPAA).

One of today’s biggest business challenges is to understand how technology and, in particular, data processing inside as well as outside a company works.

Some cloud enterprises have started experimenting with technologies such as placing server centers under water in order to reduce cost of cooling that makes up a significant part of the running costs of a server center.

\textsuperscript{219} Hadoop is an open-source software framework used for distributed storage and processing of very large data sets. It consists of computer clusters built from commodity hardware. All the modules in Hadoop are designed with a fundamental assumption that hardware failures are a common occurrence and should be automatically handled by the framework.

\textsuperscript{220} For example IBM, Hortonworks and EMC Pivotal have implemented such measures to ensure a better flow of data between their service offerings.
Placing these server centers into international waters will create further questions as to the applicable data protection laws to these centers.

II. Regulatory Gap

The main privacy protection framework has been developed in the 1970s and is ill suited for the new capabilities that Big Data provides. This includes the obtaining of consent, as well as the balancing of the risks to the individual. Furthermore, the definition of human subjects used in the Federal Policy for the Protection of Human Subjects further creates challenges, as it is very narrow.221 This definition requires some form of interaction or intervention by the researcher with the data subject. However, such interaction often is no longer required where the data is pulled from, for example, social media services.

Many of these regulatory challenges push the interpretative boundaries of current data protection and other laws that apply to the intersection of law and technology. But the legislative organs are either lacking the political will to face these challenges or the result of the deliberative process is too far removed from what the specialists have recommend to be effective in practice. Closing any regulatory gap that arises must be as expediently as possible in order to provide the market participants with the legal certainty they require in order to understand what compliance measures are required and how they must adjust any new service offering. Antiquated laws can thus hinder the development of new technologies and market entry by startups and other smaller innovative enterprises.

III. Behavioral Targeting

Information about millions of people is collected for various purposes, including behavioral analysis and targeting. Facebook collects information

221 Federal Policy for the Protection of Human Subjects, 7 C.F.R. pt. 1c, 10 C.F.R. pt. 745, 14 C.F.R. pt. 1230, 15 C.F.R. pt. 27, 16 C.F.R. pt. 1028, 24 C.F.R. pt. 60, 28 C.F.R. pt. 46, 32 C.F.R. pt. 219, 34 C.F.R. pt. 97, 38 C.F.R. pt.16, 40 C.F.R. pt.26, 45 C.F.R. pt. 46, 49 C.F.R. pt. 690, 49 C.F.R. pt. 11 (2015).
about at least 1.5 billion people, and Google reaches 90% of Internet users worldwide.

Additionally, a number of unknown companies process millions of personal data records on a daily basis. A wide range of companies is involved in behavioral targeting, using a complex network of data flows. Essentially, a system follows an internet user’s steps through the web and displays targeted advertisement.222

Data protection laws seek to limit such a privacy infringement by setting strict boundaries to personal data processing. But analytics companies are becoming more and more creative in avoiding the use of personal data, thus falling outside the scope of these laws. However, the European Data Protection Authorities, cooperating in the Article 29 Working Party, are of the opinion that behavioral targeting generally entails personal data processing because companies use the data to single out individuals. The Working Party is an independent advisory body and publishes opinions on the interpretation of data protection law. Although their opinions are not legally binding, judges and Data Protection Authorities often follow the Working Party’s interpretations.223

At the core of determining whether an analytics processing operation requires the fulfillment of the EU data protection law lies the definition of personal data. This applies to (i) any information (ii) relating to (iii) an identified or identifiable (iv) natural person.224

The core issue in making the determination of personal data relates to the third element of identifiability. This conclusion heavily relies on the underlying technology and its precise application to a given scenario. Court judgements setting out, for example, that IP addresses are personal data are not helpful in this regard, as the identifiability relies on who has the data necessary for identification. In the IP scenario, this information is only accessible and known by the Internet Service Provider but not to the search

222 Borgesius, 256–271.
223 Gutwirth and Poulet, 570 et seq.
224 See Article 29 Working Party, ‘Opinion 4/2007 on the concept of personal data’ (WP 136), 20 June 2007.
engine or marketing company. Thus, a more focused approach, taking into account of the actual identification capabilities and the service provisioning, should be taken by supervisory authorities and regulators.

IV. Government Data Release

Big Data is not only a challenge for private enterprises and their compliance with data protection law but also for public agencies which have collected a large amount of data over decades. Only recently with the use of new technologies such data can now be processed in the Big Data context. Furthermore, the low costs of storing data incentivize such behavior. However, as the government collects data under law that allows the collection for a public purpose, the disclosure of such information to private parties that otherwise probably would not have access to the data from individual users creates many data protection challenges.

1. United States

1.1 Government Data Collection

In order to promote transparency and accountability, governments are increasingly releasing a wide variety of data they collect as part of their public function. In the US, these government data releases can be grouped into four broad categories, which consist of:

- Freedom of Information and Privacy Act requests;
- Traditional public and vital records;
- Official statistics;
- E-Government and Open Government Initiatives.

Based on the nature of this data, it can be extremely important for research and business decisions, since the data allows a better insight into human behavior. The main question in this context is how a meaningful privacy

---

225 Altman, Rogerson, 835 et seq.
protection interest can be achieved. The lack of a clear framework for the protection of personal data may lead to a restrictive disclosure of privacy sensitive data.\textsuperscript{226} When privacy laws are circumstantial and open to interpretation, the disclosure does not scale; thus the process of releasing information becomes a highly labor intensive task that is slow and costly.\textsuperscript{227} De-identification of data by traditional statistical techniques has often proven to not provide the required privacy protection.\textsuperscript{228}

1.2 Freedom of Information

When data is released under a freedom of information (federal law) request, the releasing agency is not required to notify or give the person whose information is made available a possibility to object to the disclosure. At the state level, sometimes this right to object is given in narrow circumstances. Furthermore, the system is set up to penalize the employees that do not release information which should be released.

In contrary circumstances when data should not have been released, no such penalty exists.\textsuperscript{229} However, the Privacy Act of 1974 generally prohibits disclosure of records by federal agencies without the data subject’s consent. If a FOI exception applies, the corresponding Privacy Act exemption must be cited and the data released with discretion.\textsuperscript{230} Although there are exceptions to the disclosure such as for national security reasons or the data being related to internal personal records, most of the information can be requested.

In deciding to release records, a balancing test has to be carried out. Thus, the wider a release request is framed and the higher the likelihood of a

\textsuperscript{226} Schwartz, Solove, 1815 et seq.

\textsuperscript{227} Schwartz, Data Processing and Government Administration: The Failure of the American Legal Response to the Computer, 1321 et seq.

\textsuperscript{228} Ohm, 1702 et seq.

\textsuperscript{229} 5 U.S.C. § 552(a)(4).

\textsuperscript{230} Ibid § 552(a)(b)(2).
person being linked to the information is, the more the balance favors disclosure. However, practice has shown that case law has little effect on the determinations of officials. Rather, their background and training affect the decision-making. Commonly redacted information includes social security numbers, data and place of birth, as well as medical history.

However, in practice the rights of an individual to enforce his or her rights under the Federal Privacy Act remain limited through statutory hurdles and low damages, which ultimately do not provide the required incentive to change public agency behavior.

1.3 Open Access

In order to use the government data efficiently, analytics enterprises require open access to the electronic information, which enables the quick access and regular updating of their data pool. Previously, this has not been the case for all types of data, as various agencies or arms of governments have different systems and procedures on the disclosure of the data. This sometimes leads to unwanted restraints on the data disclosure, such as requiring the supply of a new hard drive for copying the data. Positive examples are the federal agencies that must frequently store requested records in electronic reading rooms or libraries and new online platforms for receiving access.

Today, there is an entire industry dedicated to compiling information from public records, adding value and creating new service by combining the data with other data. One of the biggest providers of such a service is

---

231 See e.g. Arieff v. U.S. Departement of Navy, 712 F.2d 1462, 1467 (D.C. Cir. 1983).
232 See e.g. BeVier, 495.
233 See e.g. Associated Press v. U.S. Department of Justice, 549 F.3d 62, 65 (2d Cir. 2008).
234 Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 596.
235 Wong, FOI.1ing NYC’s Taxi Trip Data, Blog (18 March 2014) <https://www.chriswhong.com/open-data/foil_nyc_taxi>.
236 See e.g. FOIA library, U.S. Census Bureau, <http://www.census.gov/about/policies/foia/foia_library.html>.
LexisNexis with access to over 36 billion public records. Although there are some limitations to the disclosure of data, such as through the Driver’s Privacy Protection Act, they can be circumvented by the person’s consent. This consent may be included in the fine print when the individual signs up for a rewards card, for example.

Statistical data is also an area of concern for privacy advocates, as it does not appear to identify individuals based on the measures that must be taken under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA).\(^\text{237}\) However, by combining the statistical data with other data sets, identification becomes possible again.

2. **European Union**

Generally, the right to privacy has a much higher value in the EU than in the US. Traditionally, the US places a strong right on the public to „keep a watchful eye on the workings of public agencies“\(^\text{238}\), which is the basis for public disclosure of court records and other data.

Generally, surveillance measures are only accepted by the Member State courts in an individual case based on evidence presented by the prosecutor. The prosecutor must show that there are no other reasonable means available to obtain the information sought and specify the duration for which the surveillance is granted. Based on these facts the judge will balance the competing interests of the state against the rights of the individual to determine whether a warrant for certain surveillance measures will be granted.

With regard to foreign surveillance the extent of potential measures is not public. However, based on the information leaked by Edward Snowden it

\(^{237}\) See Office Management and Budget, Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2001 (CIPSEA) 2006, <https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/proposed_cispea_guidance.pdf>.

\(^{238}\) Nixon v. Warner Communications Inc. 435 U.S. 589, 598 (1978).
has become clear the UK has also extensive surveillance measures in place both nationally as well as internationally.

E. Discrimination Based on Data

The ability to discriminate against individual persons or groups of people by using technology such as cloud computing, Big Data and IoT presents a high risk for any enterprise. Often the discrimination is not fully noticed as systems may identify patterns that are used for targeted advertisement but result in an effective discrimination of a group of people based on his or her race, color, sexual orientation, age, etc. The laws with regard to this conduct may allow the affected individuals to bring discrimination lawsuits, which can cost start-ups as well as large corporations millions of dollars. Thus, in addition to potential violations of data protection and other laws regulating the use of certain types of data, the result of the conducted processing operation and its application to the business may also violate anti-discrimination laws.

I. Big Data

1. Key Elements

The White House has highlighted the potential for discriminatory Big Data analytics, as well as its ability to reduce discriminatory practices when applied correctly. In particular, the report includes the fact that predictive analysis can be a barrier to entry and thus hardwire discrimination. For example, such analytics are already used for credit scoring, which automatically rates the risk of a single mom living in a low-rent neighborhood higher than a single male in an expensive district. However, in reality the single mom may be much more prudent in her finances than the single male who spends all his money and lives above his financial capabilities.

---

239 Smith, Patil, Muñoz, Big Risks, Big Opportunities: the Intersection of Big Data and Civil Rights, White House <https://www.whitehouse.gov/blog/2016/05/04/big-risks-big-opportunities-intersection-big-data-and-civil-rights>.
Thus, when machines make decisions, human control and checks are essential.

Furthermore, when designing such algorithms accounts of biases must be taken. On the positive side, Big Data can also act as a tool to identify bias by comparing a huge amount of decisions and predictions and contrasting these to certain characteristics. The main categories which can create discriminatory effects are (i) based in the data that is used as input to an algorithm and (ii) the inner working of the algorithm itself.

When the discrimination results from the data, the source is either:

a) Poorly chosen data in which the designer of the system selects what data is used but omits other data. This causes a discrimination against the omitted class. Such situations can occur when certain data is deemed not to be required for the decision but not including it results in a discriminatory result.

b) Incomplete, incorrect, or outdated data, which can be created by a lack of technical rigor and comprehensiveness in the data collection. For example, the data collected is not updated regularly even though it changes frequently.

c) Selection bias that results in the data sample not being representative of a population and thus discriminating against the omitted group.

d) Unintentional perpetuation and promotion of historical biases derived from a feedback loop, causing a bias in inputs or results of the past to replicate itself.

Furthermore, the design of algorithmic systems and machine learning can also facilitate discrimination through:

a) Poorly designed machines systems, which facilitate the finding of information. If such systems are not kept up to date and account for historical biases within the data or algorithm used, they may produce discriminatory outcomes.

---

240 Executive Office of the President, 45.
b) Personalization and recommendation services that narrow instead of expand user options. For example, when a user receives targeted advertisements automatically, market segments are excluded, and the person is no longer aware of this information.

c) Decision-making systems that equate correlation and causation. This can happen when a system thinks that because two factors occur together, they must be in a causal relationship.

d) Data sets that lack information or disproportionately represent certain populations, resulting in imprecise algorithmic systems that facilitate discrimination because of the flawed input.

2. Credit Scoring

With the increase in scoring capabilities through Big Data, the risk that a person who would otherwise have a good credit will be classed as unscorable has risen. Today, electronic systems rely on the data they receive from other lenders in order to produce an automated credit decision. However, those that do not have loans will not be able to receive a score, as there is no data on file and thus will not be granted a loan based on a lack of data. As this affects mostly African-Americans or Hispanic-Americans, discrimination is created if no other credit assessment method is offered to account for their unique situations.\textsuperscript{241} However, with the rise of Big Data, new methods in assessing credit risks can be developed that take into account new data sources that do not limit the assessment to current loans and past loans. This fact will benefit low-income borrowers, as with additional utility and telephone bill data 70% of the unscorable files would become scorable.\textsuperscript{242}

3. Employment

In addition to the commonly accepted areas of Big Data such as the finance industry, Big Data is also used increasingly in the employment context. A

\textsuperscript{241} The Consumer Financial Protection Bureau Office of Research.
\textsuperscript{242} Turner, Walker, Chaudhuri, Varghese, 23 et seq.
company seeks to find the perfect candidate that not only has the technical skills the company is looking for but also the cultural values of the company and the nature necessary for the role. Such analytical tools have found widespread use today in the pre-selection process. However, often the way in which they work or how the final list of candidates is computed remains unclear.

Additionally, by selecting people based on keywords and assumptions related to their personalities, diversity is reduced when the company only seeks out people that are like the employees they already have. Furthermore, factors such as the length of time at a job could discriminate against individuals who have been unemployed for a longer period previously.\textsuperscript{243}

However, such systems also have the ability to reduce “affinity bias”, as the system only provides information on the applicants that all meet quantifiable criteria. Furthermore, new systems that run in the cloud allow for a comparison of salaries across various corporate entities in order to ensure equal pay and non-discrimination.\textsuperscript{244}

4. Higher Education

Potentials for unwanted outcomes of Big Data processes are also present in the context of higher education. Data that is collected through the enrollment process as well as in class can be analyzed to determine whether a particular student requires some form of assistance or tailored study. However, the same tools can also be used to discriminate against such students by denying admission or other opportunities.

In particular, the US college system, which is very expensive and requires students to take out huge loans, can benefit from data analysis. For the first time, parents are able to view a nationwide comparison of colleges based on an analysis of income after graduation, dropout, loan repayment, as well as other data that Big Data tools can help to understand. This enables parents and students to determine at what college they receive the most

\textsuperscript{243} Executive Office of the President, Big Data: A Report on Algorithmic Systems.

\textsuperscript{244} For example the cloud solution by SaaS HR provider allows for such measures.
benefit for their money. They are then able to make an informed choice on a college based on their individual circumstances and preferences.

Big Data technology can also help students learn more effectively through tailored instructions based on their level of knowledge and areas that need more attention. Georgia State University has rolled out a program in 2013, which tracks over 800 risk factors for each student on a daily basis. It aims at identifying problems that then can be resolved through proactive measures. This approach has resulted in an increase in graduation rate of 6% and has significantly benefited underprivileged groups, including black and Hispanic students. Additionally, this tailored care results in faster graduation and thus reduced the financial costs for the students.

In the context of admission procedures, additional data may help in the selection process. However, it can also disadvantage poorer applicants, since parent income is an indicator for college outcomes.

5. **Criminal Justice**

The use of Big Data in the context of law enforcement has significantly increased in the US over the last decade. Technologies that help to catch and identify criminals can also be used to make law enforcement accountable to their communities.

Modelling systems can refine the understanding of crime hot spots and link crime data to other factors in order to identify measures that should be implemented in the community to reduce violence and other risk factors. De-identified police data as well as other contextual data can be used to carry out predictive analyses, which will enable the prediction of areas and times in which the risk of crimes is highest. The police is then able to

---

245 Kurweil and Wu, Building a Pathway to Student Success at Georgia State University, Ithaka S&R, <http://www.sr.ithaka.org/publications/building-a-pathway-to-student-success-at-georgia-state-university/>; Marcus, Colleges Use Data to Predict Grades and Graduation, The Hechinger Report December 10, 2014 <http://hechingerreport.org/like-retailers-tracking-trends-colleges-use-data-predict-grades-graduations/>.
dispatch additional units to these areas to prevent criminal activities. These proactive steps have resulted in large reduction of reported crime.

In order to reduce the risk of singling out particular communities based on individual characteristics, such as race, sexual orientation, religion or income level, the systems and algorithms must be assessed against the risk that historical data presents. Feedback loops are able to reduce these risks, but they must be carefully constructed. However, the core risks lie in the data sources, which are often not up to data or lack the required richness and are partially non-complete.

II. Use of Personal Data in Big Data Processing

The above detailed examples of how Big Data is used are, for the most part, not inhibited by data protection laws in the US. However, in the EU, the extensive privacy protection framework as well as the data protection laws both on EU and national levels place strong limitations on the use of personal data for Big Data analytics. If the processing is for public purposes or in the public interest, EU Member States are granted some leeway in implementing their own law that ensures the protection of personal data while allowing for this data to be utilized for the benefit of the Member State.\textsuperscript{246}

Although the EU is increasing its stance on a digital economy, Member States are still slow to adopt new technology in their public sectors.\textsuperscript{247} Often the structures are ill equipped to new changes, and the authorities lack the insights necessary to benefit from new technologies such as Big Data. Additionally, the data collection in Europe is far more limited than in the US, and thus the data required for a detailed and reliable analysis is often not available.

Open government is a core concept both in the EU as well as in the US. However, in the EU, information often is not released in an electronic form,

\textsuperscript{246} General Data Protection Regulation, Article 6.
\textsuperscript{247} Estonia is a noteworthy “anomaly” in this regard as nearly all interactions with the government can be conducted electronically with an electronic passport system.
which would allow third party vendors to design and implement services that make use of such data. This is partially based on data protection law, aiming at protecting personal information when the release of such data is sought by the government. In these cases, the data must not contain any personal data that would allow the identification of an individual. Only when the balancing test between the interests of the public and the data subject whose data is contained in the data to be disclosed favors a disclosure can the information be released. This is an individual assessment and cannot be conducted by automated means, which results in much of the information not being disclosed unless a person seeks access to it under a freedom of information request.\textsuperscript{248}

Thus, in order to use information that is collected and produced in the public sector more efficiently, rules must be implemented to allow public agencies to increase their efficiency. Naturally this data should only be used internally and not given to commercial enterprises. Any results of the Big Data processing activities must be made subject to an independent re-evaluation procedure, which ensures the integrity, accuracy, and reliability of the data and also the system that compute any result of a processing operation.

Linking all sorts of government data such as health, financial data and personal characteristics together increases the overall precision and prediction capabilities of the data. Thus, the line is blurring between the various types of data which will in the future present significant legal questions in particular in the US, as these types of information are governed by individual and specific regulation. One dataset containing health and financial data would, for example, be subject to HIPAA\textsuperscript{249} as well as the Gramm-Leach-Bliley Act, Fair Credit Reporting Act\textsuperscript{250} and other relevant legislation. Managing the use and interaction of the data as well as the results of processing and analysing the data becomes a complex matter, as some of

\textsuperscript{248} Freedom of Information Act, Pub.L. 89-487, 5 U.S.C. § 552.
\textsuperscript{249} Health Insurance Portability and Accountability Act, Pub.L. 104–191.
\textsuperscript{250} Fair Credit Reporting Act, Pub.L. 114-38, 15 USC § 1681.
the recipients may not generally be regulated by any of these laws yet will face additional burdens when using or receiving such information.

In order to be able to address the issues created by Big Data, a better understanding of the cloud infrastructure underlying such Big Data calculations is necessary. A legal as well as a contractual framework regulating cloud provider activities must be in place to ensure a minimum data protection level is met before the further complexities of Big Data are added to the mix.

However, the reality is such that the data protection level achievable before the advancements of the cloud and Big Data is no longer practicable, because the technological ease of a privacy infringement has exceeded expectations and, to some extent, gone beyond the ability of governments to regulate effectively at national level. It is therefore sensible to start tackling these challenges by focusing on regulating the personal data transactions at the lowest level of the cloud first before addressing the technologies utilizing the cloud further up the service hierarchy.

A point of criticism has been the lack of guidance on how broadly formulated privacy principles on which many countries agree can be implemented. The local implementation of broad horizontal privacy principles (in accordance with national interests such as human rights, security and cost) has reached its limits with the emergence of new Web 2.0 systems. Currently the GDPR could set the international data privacy standard, as there is a lack of movement on the international level by the UN to

---

251 For the data protection aspects and the security challenges see Cloud Security Alliance, 11.
252 For a discussion of user privacy perception in the context of mobile phones see Fife and Orjuela, 1.
253 Attempts at implementing privacy policy into technology are being undertaken by ENISA. However the ineffectiveness of the currently applied anonymization technologies in the context of Big Data are questionable (see Danezis and others, 37). The Article 29 Working Party has also published a statement in this regard: Article 29 Working Party, Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU (WP 221, 2014).
254 De Hert and Papakonstantinou, 271 et seq.
pass appropriate measures. Parallel to the delayed regulation, technical think tanks have emerged with the purpose of finding technical solutions to the privacy issues created by technologies such as the Internet of Things, cloud computing and Big Data. But, the legislative process is too slow to keep up with technological development, thus emerging privacy standards will be driven more by technology than by regulation. Customer demand for privacy will also play an important role in shaping the future of how privacy is ensured.

Regarding the GDPR and current developments in the EU the question arises whether the consent and collection focus is still a prudent solution as Big Data allows for all sorts of identification scenarios which are not covered by the scope of the GDPR at the time of collection. They only arise later in the context of processing for statistical purposes. Thus, the legislator should place a stronger focus on protecting data subjects irrespective of whether they have consented to an initial collection. As Big Data processing operations make out the bulk of processing in the cloud, emphasis must be placed on these questions and on ensuring a harmonization of the rules regarding obligations in the context of processing for statistical purposes.255

F. Compliance and Risk Mitigating Measures

The increased international regulations have led to higher compliance costs as well as to a major complexity in international data transfers. Companies are increasingly facing requirements they currently are not able to meet because of the way in which their data collection is set up.256 Thus, becoming compliant with all the various data protection laws requires a

---

255 Article 89 GDPR allows Member States much leeway in imposing their own requirements.

256 For example, these particular issues arise in the context of data protection laws and the combination of Big Data, resulting in a higher degree of identifiability of a person. The initial collection of the data may not have required consent, however, based on the nature of the processing conducted at a later time and the result of such processing, the person’s consent as an identifiable data subject is required.
step-by-step approach taking into account the areas in which the risk is the highest and addressing them first.

As a consequence of developments towards a more active inclusion of different stakeholders into the rule-making processes, many issues such as the models of data privacy governance, their convergence, the need for globalized data protection standards, and the regulation of trans-border data flows need to be reflected anew.

I. Privacy Management Programs

The respective refinement and adaption of privacy rules can be carried out through the improvement and the practical implementation of privacy management programs that enable enterprises to satisfy the regulators and supervisors of their compliance with privacy standards. Such programs also have the potential to act as a strong marketing instrument since they send a signal that businesses care about the privacy of their customers and stakeholders by attempting to reduce the risk of a privacy breach.

The content and structure of such programs can be quite flexible, thus enabling the necessary adaptation to the given circumstances. Nevertheless, a stronger coordination on the international level as to privacy standards seems warranted in light of the great differences in protection levels. In particular, the cooperation among data protection authorities from different states must be enhanced in order to prevent violations.257

1. Achieving Data Protection Compliance

Effective data security starts with assessing what information the company has and identifying who has access to it. Understanding how personal information moves into, through, and out of the business and who has—or could have—access to it is essential to assessing security vulnerabilities. In order to determine the best way to the protection of personal data, the data flows must be understood.

257 Galetta and Kloza, N 1 et seq.; Weber, Internationale Trends bei Datenschutz-Managementsystemen, 31 et seq.
A first step is to establish an inventory of all computers, laptops, mobile devices, flash drives, disks, home computers, digital copiers, and other equipment to find out where the company stores sensitive data. Also, the information should be inventoried by type and location. Personal data is stored throughout the business in a number of ways — through websites, from contractors, from call centers, and the like. No inventory is complete until a search has been conducted at every place where sensitive data might be stored.

Once the personal data that is present in the company has been assessed, the data flows into, through and out of its various IT systems must be monitored and assessed against the processing justifications necessary under the applicable law. The best approach is to determine what information is actually necessary to provide the service and not to collect any data that is not essential. However, in light of the decreasing costs of data storage, many companies take a different approach and collect all data they are able to. The ultimate goal is to use this data in the future for yet unknown purposes. This also applies to Apps running on mobile devices, which collect much more precise metadata of the user such as geolocation data. Restraints should be applied to the use of such data, as liability for data protection infringements arises very easily in this context.

A number of steps should be considered in the development of a privacy management program. The steps include the development of organizational privacy policies, standards and/or guidelines which define privacy program activities. Such activities include education and awareness training, monitoring and responding to the regulatory environment, ensuring internal policy compliance, setting up data inventories encompassing data flows, and classification.258

Additionally, data protection impact assessments and the required mitigation measures such as incident response and applicable jurisdictional re-

---

258 Danezis, Domingo-Ferrer, Hansen, Hoepman, Le Métayer, Tirtea, Schiffne, 3 et seq.
requirements must be prepared. Such assessments aim at offering the assurance that the system is compliant, which is enforced through external audits.

2. **Privacy Operational Life Cycle**

Privacy of any personal data flowing in and out of an organization must be ensured throughout the entire life cycle during which the company is responsible for it. This requires an assessment of the status quo to establish a baseline of the current level of privacy protection. Based on this information, targeted education and awareness campaigns can be created.

The success of such measures has to be monitored and further refined through internal policies upon which the employees can rely when carrying out their tasks. From a technical point, the internal data flows must be mapped and personal data storage and flow identified. Once this is done, responsibility must be attributed to a person who must ensure that this data processing operation is data protection compliant.

The risk assessment will enable the organization to gauge the exposure it has and the measure it wants to take to reduce the risk. In addition to such measures, insurance is also another tool to further shift liability. However, any insurance company will seek the implementation of appropriate safeguards to be able to calculate the risks. Thus companies must focus on fulfilling at least key privacy processing risk mitigation goals. Any strategy will be based on a gap analysis that aims at comparing the safeguards already in place with the ones set either by data protection law or by an insurance company, which in most cases are higher than the minimum protections required by law.

Compliance with privacy law does not end within the organization but also requires a detailed assessment of the contracted service vendors that often supply core data processing services. These vendors must also comply with the company’s privacy and security policies and clearly communicate who has access to what data and where it is stored or processed. In the cloud, this at least means informing the customer which processing centers are being used.
A core function of the data protection officer in particular in larger companies is the maintenance of different types of relationships both with internal and external stakeholders. These aim at ensuring efficient communication between all parties involved in the internal audit, physical and information security environment. With a view to the regulators, a strong working relationship with the Data Protection Authorities is essential in order to understand what measures are required for compliance. This task includes the scope of the contractual requirements when engaging third party vendors and their monitoring and auditing.259

Data Protection Officers, however, should not only focus on risks that arise from digital data processing but must also focus on the physical aspects of the daily operations. This includes seemingly simple questions, such as who has physical access to equipment and how physical data such as documents are destroyed. As computers have a short lifespan and are regularly replaced, storage media on these devices must be completely erased. Physical safeguards, such as the blocking of USB drive insertion, are also an important step to ensure intentional or negligent data copying does not occur, thus limiting the risk that personal data may leave the company.

3. Communication and Training

Communicating goals, values, and information pertaining to data protection and data security to employees in a coherent and receptive manner is key in ensuring the data protection management program is reflected in daily operations. This includes creating awareness of the organization’s privacy program internally and externally, as well as ensuring policy flexibility in order to incorporate legislative, regulatory, and market requirements. Furthermore, developing internal and external communication plans to ingrain organizational accountability is an important aspect to foster the implementation of company values.260

259 Staiger, Data Protection Compliance in the Cloud.
260 For example, the GDPR sets out the requirement of processing registers in Article 30.
In addition to communication in general, documents in particular require focus. For example, a company must identify, catalog and maintain documents requiring updates as privacy requirements change. The training requirement also extends not only to employees or management but also to contractors who must be made aware of the company’s privacy policies.

These privacy policies must translate into operational privacy practices, which take form in standard operation procedures covering aspects such as data creation, retention, disposal and usage as well as access controls, incident reporting and key employee contact details.

Monitoring the application of various procedures and policies ensures ongoing compliance. This can be done through the use of appropriate applications as well as through compliance staff. Any compliance measure should also be able to adjust to any regulatory or legislative change, and such changes must be quickly reported across all relevant divisions. Regular internal audits must complete any well-functioning compliance system.

4. **Response to Data Protection Issues**

Responding to various data protection issues brought to the company by external parties must be conducted in a standardized and approved form. This, for example, includes information requests to which a company is subject once it deals with individuals in the EU. If additional access is sought, the boundaries of such access and the correction or alteration rights should be clearly set out.\(^{261}\)

Overseeing and ensuring data integrity and responding to potential privacy incidents must also be part of a response plan. The goal of any compliance system should be placed on preventing harm and ensuring accountability. Such a response plan has to be set out the responsibilities and roles of key employees. However, it should not only include internal employees, but third-party stakeholder that influences the personal data processing must also be taken into account.

\(^{261}\) See for example Article 12-21 GDPR.
The communications and public relationship department must also be prepared for a wide array of incidents and for appropriately dealing with such situations. Specialized incident oversight teams consisting of IT, legal, and communication professional should be tasked with overseeing any incident and regularly meet to discuss any changes that need to be made to the incident response plan.

Managements should also include the incident response plan into their business continuity planning. However, before any response can potentially be taken, the incident must be identified. Thus, a privacy incident needs to be defined and classed based on its impact. Following this assessment, a reporting process should be set into action that enables early alarm to management. Additionally, detection capabilities such as monitoring software should be installed to alert the IT early of any potential breach. However, as incidents are not only digital but could also occur in the analog world when an employee causes a breach, appropriate procedures for such a situation should also be established.

From a legal perspective, often incident response plans that include the top management are required by law. This is also part of many insurance contracts that pay out in the case of a security breach by a hacker. Such a response should also document all actions taken in order to not only satisfy the data protection authorities but also further investigate the incident and identify the extent of the damage caused.

5. **Compliance Toolbox**

In view of the described features of privacy as a fundamental right and the application of data protection laws, businesses must develop a strategy for complying with the applicable legal requirements from many numbers of sources. (i) Organizational rules have to describe the functions of responsible persons and segregate the duties amongst them. (ii) The data protection policy must describe the security levels and the measures applied to achieve such levels. (iii) A project management needs to be implemented and conditions for user participation should be established. (iv) A data classification scheme is to be developed in order to control access rights.
(v) Adequate responsibility measures and surveillance requirements for review processes must be introduced.

Private initiatives such as the implementation of privacy management systems are particularly important, since it appears unlikely that the gap between the two major regulatory approaches for data protection regimes will be overcome in the near future. On the one hand, some countries (for example, the Member States of the European Union, Switzerland, and Hong Kong) have a comprehensive data protection model, containing core principles such as provisions on data processing and international data transfers as well as specific rules related to e-privacy measures. On the other hand, some countries have implemented a sectoral or self-regulatory/co-regulatory model (for example United States and Australia). The different approaches will most likely remain in place for the next decade, creating challenges for cross-border data flows due to the incoherent levels of protection.

Certifications under Section 5 of Chapter IV of the new GDPR also present a step in unifying data protection compliance by having an independent third party evaluate a processing operation. These certifications are accompanied by an industry-approved code of conduct, which enables standards to be created that match the requirement of a subset of processor and are tailored to their needs. Furthermore, the EU Data Protection Board (EDPB), consisting of the heads of the EU Member State data protection authorities, is empowered to issues guidelines for certain processing operations or general matters and aims to ensure a uniform application of the GDPR across all Member States.

6. **Contractual Measures**

The companies are generally quite free as to how they want to contract for various issues. This includes the data security obligations as well as all associated liabilities. Furthermore, in addition to data security, a breach of

---

262 De Hert and Papakonstantinou, 271 et seq.
263 Chapter VI GDPR.
confidentiality is a second central point that often comes up during contract negotiations. Thus, some companies have opted to have one clause for data breaches, which governs incident response as well as notification and liability provisions, whereas a lesser number of companies have taken it upon themselves to separately define a data security breach vs. a breach of confidence based on a disclosure of data. This seemingly became necessary because enterprises that could not recover under the data security clause sought alternative means to recoup their loss by arguing that the disclosure of the data to a third party was a breach of confidence for which the party was ultimately responsible.

In order to mitigate such a risk, it is advisable to either include the breach of confidence into the general liability provisions for a data breach or to separately and narrowly define such an incident. Obviously, all employees of a cloud provider should sign non-disclosure agreements. Depending on the nature of their function, they may gain access to valuable information. Some enterprises will also seek to ensure that the cloud vendor does not have access to any information and only receives the access to the extent necessary in order to facilitate the service. All interviewed cloud vendors agreed in this context that they do not want access to the data, since their core business is to offer the service they often can provide without accessing it. However, some cloud vendors, such as electronic discovery cloud platforms, necessarily require access to the data in order to improve the service. In these cases, the access must be limited to a certain number of employees. Access to all systems should also be logged as to ensure that their work environment is safe from unauthorized personnel.

Most cloud services include to some extent personal data. This is because the metadata of tasks being carried out or programs being run (e.g. app) can be used to single out an individual user. Other risks are based on the data processed in the cloud itself by the cloud customer. However, the cloud vendor will seek as little as possible access to it and leave the control for altering the data entirely in the hands of its customer. This is particularly important when later the need arises to distinguish the cloud vendor from a controller as opposed to a processor under EU data protection law.
F. Compliance and Risk Mitigating Measures

Achieving compliance in the cloud is a major challenge that requires careful preparation. This includes implementing a compliance checklist that accounts for the most important factors, such as data security. Third party IaaS vendors, such as AWS or Microsoft, will be able to support this process by offering their certifications and external compliance checks.\(^{264}\)

II. Non-disclosure Agreements and Internal Protocols

A core requirement for data protection and confidentiality is the enforcement and control of processes established to protect data within an enterprise. This includes strong non-disclosure agreements (NDA) ensuring that the data to which employees gain access is not disclosed outside the company, as otherwise it would be liable for a substantial sum of money.\(^{265}\)

Internal protocols about how to handle data, including clean desk policies, locked containers, screen protectors etc., are an integral part of any risk reduction strategy. Most data security breaches are committed by employees either negligently or intentionally. At the very least, unintentional breaches are avoidable through appropriate training.

III. Updates

Software updates present both a risk as well as an opportunity to decrease exposure. Most updates aim at patching problems that have been identified and at increasing usability of a service. On the downside, any change in a running system may create new problems and open up new intrusion vulnerabilities. Often a staggered release across multiple zones is carried out in order to identify any glitch that can be repaired before the update is rolled out to all customers.

IV. Insurance

Insurance is a basic requirement for any company offering services in the digital world. This mostly includes the basic general liability insurance,

\(^{264}\) Staiger, Data Protection Compliance in the Cloud.

\(^{265}\) Interview 6.
which may cover data breaches up to a certain limited amount. However, in practice these limited insurance sums do not cater for the loss that a data breach in the cloud could create.\textsuperscript{266} Thus, when determining what measures to take in order to fulfill data protection requirements, security breaches should also be considered and the potential loss ascertained. This information will then allow the company to seek out the appropriate level of insurance tailored to their individual risk profile.

Cyber risk is now a major threat to businesses. Today, it has become a matter of how a company manages and responds to cyber risks that counts. Companies need to make decisions on which cyber and data risks are to avoid, accept, control, or transfer. Data not properly managed can quickly become a liability and an expensive direct cost to a company. When a data security breach or a cyber-attack happens, the company needs comprehensive cyber insurance protection to help it to respond. These insurance schemes are available up to 500 million USD with the average claim being around 700 000 USD.\textsuperscript{267}

Coverages currently available include: Network Security Liability, Privacy Liability (Including Employee Privacy), Breach Response, Privacy Regulatory Defense, Fines and Penalties, Errors and Omissions, Forensics, Multi-media Liability, PCI Fines and Penalties, Network Business Interruption, Data Loss, Cyber Extortion and Cyber Terrorism. These insurances come also with access to a 24/7 team of incident response experts. Often, insurance companies also offer complimentary cyber risk assessments as part of their own risk and premium evaluation.

The number of claims based on data breaches has steadily risen and often covers not only financial data, which is mostly securely guarded, but also employee records. For example, employee records, including exit interviews and disability applications, were leaked from the Little Eagle Casino.

\textsuperscript{266} Weber and Staiger, Legal Challenges of Trans-border Data Flow, N 12 et seq.

\textsuperscript{267} See e.g. Cyber Data Risk Managers <https://databreachinsurancequote.com/request-a-cyber-insurance-quote/>.
in Canada.\textsuperscript{268} Others include a data breach when an employee copied 600 health files to a flash drive that was subsequently lost.\textsuperscript{269} However, where the misconduct is intentional and based on a lack of sufficient protection tools and procedures, the insurance company is unlikely to cover the incident. Not even in hacking cases are companies immune, as shown in the case of the Israeli company Cellebrite from which over 900GB of data were stolen.\textsuperscript{270} Thus the need for insurance persists across all business sectors even in industries which deem themselves to be sufficiently protected based on their particular expertise with data security.

\section*{G. Ensuring Data Security}

Cyber security has long been a growing area of concern for many scholars as well as enterprises seeking to ensure that data is not accessed by a third party that has no rights to the data. Often rules in various jurisdictions offer precise guidance on certain data protection aspects but only vaguely highlight the requirement of cyber and data security.\textsuperscript{271} At one point, the concern of legislators was the risk of deciding on a technology by imposing fixed requirements. This may defy the purpose of data security, since the legislator does not have the capacity or knowledge to determine what security technology is most appropriate. Such technologies are also undergoing rapid change and may be out of date after a short period of time. Thus, enterprises must be able to adjust their security measures in accord-

\begin{footnotesize}
\begin{enumerate}
\item Global News, Grey Eagle Casino employee information leaked in major privacy breach, \url{http://globalnews.ca/news/3206136/grey-eagle-casino-employee-information-leaked-in-major-privacy-breach/}.
\item Data Breaches Net, Complete Wellness notifies 600 patients after employee misconduct results in lost PHI, \url{https://www.databreaches.net/md-complete-wellness-notifies-600-patients-after-employee-misconduct-results-in-lost-phi/}.
\item Motherboard, Hacker Steals 900 GB of Cellebrite Data, \url{https://motherboard.vice.com/en_us/article/hacker-steals-900-gb-of-cellebrite-data}.
\item See Weber and Studer, 716 et seq.
\end{enumerate}
\end{footnotesize}
General Measures

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA)\(^{272}\) states that the information must be protected by safeguards appropriate to the sensitivity of the information. The nature of the safeguards may vary depending on the sensitivity, amount, format, and distribution of the information as well as its storage method. The methods are broadly described and include physical, organizational and technological measures. Such a principle-based approach is also applied in the US and Australia.

With the flexibility that such an approach provides comes the lack of precision required by various industries to draw the legal certainty for their compliance measures. In order to address these issues, supervisory authorities have published guidance documents and reports based on previous cases. For example, the FTC published on 29 July 2016 a guidance on what are required in order to meet the level of reasonable and appropriate data security practices.\(^{273}\)

In the US, the data security question is governed by the three-prong unfairness test from the Wyndham case.\(^{274}\) This includes a cost-benefit analysis that considers a number of relevant factors, including the probability and expected size of reasonably avoidable harms to consumers given a certain level of cybersecurity and cost to consumers in taking such measures.\(^{275}\)

Thus, the test remains as to whether the measures taken by the enterprise are reasonable in light of all the facts. In Canada, the focus is placed on

\(^{272}\) Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.
\(^{273}\) See LabMD Inc. v. Federal Trade Commission, (11th Cir. Sept. 29, 2016).
\(^{274}\) FTC v. Wyndham Worldwide Inc., 799 F.3d (3d Cir. 2015).
\(^{275}\) Ibid, N 255.
G. Ensuring Data Security

appropriate safeguards. Whether these two standards differ in their application must be examined with reference to the respective national law. However, on their face they appear to be very similar. In the UK, this standard is lower than in Canada as the UK Data Protection Act only requires appropriate measures taking into account the state of technological development and the cost associated with implementation. The US FTC guidance also includes a cost-benefit analysis in light of the required investment and its outcome.

In the LabMD report, the FTC focused on the following factors:

- Whether the data being processed is sensitive data that requires awareness within the company;
- Whether there are appropriate processes, procedures, and systems to handle information security risks and whether there is internal or external expertise available on this topic;
- Whether a safeguard assessment is in place that offers the required level of safeguards for any processed personal information;
- Whether a risk balance is in place which adopts safeguards in accordance with the risk.

Thus, when an enterprise collects a large number of sensitive personal information, a governance framework is necessary that takes account of the abovementioned factors. In the Ashley Madison case, the FTC highlighted that the company lacked documented policies and practices that would have provided clear security expectations. Furthermore, a clear risk management process was also lacking. Without such a regular assessment, appropriate measures that must be taken in order to reduce security risks cannot be determined. If necessary, such expertise must be acquired externally and should be based on the nature and volume of the processed information. Importantly, the documented risk management framework

276 PIPEDA Case Summary 2016-005 Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner, para 10.
must include a guidance on how the enterprise determines what security measures are appropriate to a faced risk.

Interestingly, the FTC observed that the company had been evaluating acquiring external expertise on data security but that it ultimately decided against it. It remains to be seen whether such an evaluation of a need will play a role in assessing the measures taken.

Some practices have become the common standard and must be implemented by all organizations handling personal information, such as multi-factor authentication. This technology consists of information the user knows, something that is in the user’s possession and something the inherent to the user. Many systems only focus on the knowledge part and lack the two other elements.²⁷⁷

Key and password management practices must also be adjusted to ensure third party access to the data is impossible. This includes not to store such credentials on shared drives and to protect the internal systems sufficiently. Importantly, employees should be limited in their ability to access keys and never store any login details in an unencrypted fashion. Once a hacker gains access to a system by exploiting a human error, he or she can in most cases move very freely between systems as the authentication has already taken place.

²⁷⁷ Ibid, paras 72, 73, 80.
In addition to the requirements under general data protection law, special legislation sometimes applies, such as the HIPAA which requires the identification of risks and vulnerabilities as part of a general compliance procedure. From a technological side, the Nation Institute of Science and Technology provides guidelines regarding risk management in information technology systems. As the chart below illustrates, data security violations are often based in employee and third party access to the premises and not by outside hackers.²⁷⁸

²⁷⁸ Compliance and Safety LLC < http://complianceandsafety.com>
Today, the following measures should be the basis of any risk assessment:\footnote{Beardwood and Bowman, 171.}

- Intrusion detection systems;
- File integrity monitoring;
- System penetration testing;
- Updated virus scanner and regular checks;
- Manual inspections with written protocols;
- Effective firewall including data flow monitoring.

The higher monitoring requirements create challenges with regard to user privacy because the monitoring will in one way or another touch upon the transmitted data in order to assess whether the data flow is legitimate. Thus, although such a measure aims at increasing security, it may well affect privacy.

Although the guidance provided is very basic, it is a first step towards more certainty. However, any of the measures will affect the security measures taken by companies offering goods or services online. Often corporate culture is a big part of how management and the enterprise in general approach security issues and whether the will to set sufficient resources aside for such measures is present.

II. Security and the Internet of Things

The Internet of Things has further increased the complexity of data collection, transfer, and storage. In this context, new and exciting technologies are making life much easier whilst at the same time collecting an increasing amount of data about the persons within the surroundings of the device.
The IoT adds new security dimensions to consider. For example, an insecure connection could give a hacker access not just to the confidential information transmitted by the device but to everything else on a user’s network. Furthermore, in the IoT, the risk is not just based in the disclosure or deletion of data. If the home automation system is not secure, a criminal could override the settings to unlock the doors. For example if a hacker were able to remotely recalibrate a medical device – e.g. an insulin pump or a heart monitor – serious body damage could be caused.

Thus, when vetting such devices, due attention must be paid to the security measures implemented. Based on the complexity of IoT, there is no singular checklist that would take into account all the various forms which such devices could take.

A key security challenge in the IoT context is the increase of the overall exposure\textsuperscript{280} to malicious attacks,\textsuperscript{281} as compared to isolated (i.e. non-connected) systems. This may be attributed to the following factors:\textsuperscript{282}

Due to the ease and low cost of developing IoT devices as well as to the high adoption rate of smart connected devices, the IoT ecosystem will continue to steadily grow in volume and variety in the coming years.\textsuperscript{283} Various companies and organizations have published projections regarding the number of things that will be connected to the Internet in the coming years. A conservative prediction by Gartner, highlights that the number of networked devices in use worldwide will reach 20.8 billion by 2020.\textsuperscript{284} Cisco’s estimates are around 50 billion IoT connections by 2020.\textsuperscript{285} Huawei projects that such connections will hit the 100 billion figure by 2025.

\textsuperscript{280} A system’s attack surface can be defined as the subset of its resources that an attacker can use to attack the system (see Manadhata and Wing, 4)
\textsuperscript{281} Ernst & Young, 8 et seq.
\textsuperscript{282} Weber and Studer, 719.
\textsuperscript{283} McAfee Labs, 21
\textsuperscript{284} Gartner Press release.
\textsuperscript{285} See the Cisco White Paper, 1.
While the exact numbers are uncertain, the overall picture is clearly one of significant growth. The direct result is that there will be a massive amount of Internet-enabled devices operating dynamically that will require a sufficient protection. Due to the fast development of the IoT that occurred without appropriate consideration for security issues, smart devices are inherently insecure. A 2015 study by Hewlett Packard showed that 70 percent of IoT devices contain serious vulnerabilities. These vulnerabilities stem in particular from the following:

- Lack of transport encryption: Many IoT devices are simple “unit-taskers” and all devices have cost, size, and processing constraints (additional processing power adds cost). This means that most devices will not support the processing power required for strong security measures and secure communication, such as encryption (e.g. an 8-bit microcontroller, the function of which is merely to switch lights on and off, cannot support the industry standard SSL to encrypt communications) and may transmit data in clear text. This is, of course, particularly problematic in the IoT context, given the massive amounts of data that are being transmitted between smart devices, the cloud and mobile applications.

- Insufficient authentication and authorization: Authentication/authorization can be insufficient due to poor password requirements, careless

---

286 See Huawei, 43.
287 Internet Society, 2.
288 Khoo, 709.
289 Hewlett Packard, Internet of Things Research Study.
290 Symantec White Paper.
291 Verizon, 63.
292 Ibid.
293 Shackelford, Raymond, Balakrishnan, Dixit, Gjonaj, Kavi, 9.
use of, lack of periodic password resets and failure to require re-authentication for sensitive data. Weak authentication and authorization compromise the entire IoT system.  

- Insecure Web interface: Security issues with the web interface include persistent cross-site scripting, poor session management and weak or plain default credentials (which can be exploited by enumerating accounts until access is granted).

- Insecure software and firmware: due to resource constraints, most IoT devices are designed without the ability to accommodate software or firmware updates (which would add cost). As a result, vulnerability patching is difficult. This is problematic since it is “virtually impossible” to design vulnerability-free software. In addition, where updates are available, many devices do not appear to use encryption for software updates downloads. Hence, the explosion in the number of connected devices, coupled with the IoT’s numerous security deficiencies is shifting the security paradigm from hardware to the networks that process the devices. In terms of security, each thing is a potential entry point for an attack, which creates a great imbalance in what appears to be a cybersecurity arms race: While defenders must secure every single part of the ecosystem, all that is needed for an attacker is a single entry way into the network. As such, “anything networked becomes a link in the long chain which is only as strong as its weakest link”.

The FTC has outlined a few factors that should be considered, including:

---

294 The Open Web Application Security Project (OWASP) of the Top 10 Insufficient Authentication/Authorization, https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization.
295 Gwarzo, 3.
296 Russell, Data Security Threats to the Internet of Things, <https://www.parksassociates.com/blog/article/data-security-threats-to-the-internet-of-things>.
297 Choi, Fershtman, Gandal, 869.
298 Ibid, 870.
299 Gwarzo, 3.
– Encouraging a culture of security within the enterprise, including the designation of a responsible security officer and training of staff;

– Taking into account security as a core component in the design of the device (security by design);

– Implementing an in-depth defense strategy at every layer of the service provisioning and data access will also increase overall security and limit the potential damages that an intruder could create;

– Allocating the resources based on the level of risk involved, starting with the greatest risk, and allocating resources to subsequent risk mitigation measures when they become available;

– Avoiding default passwords unless consumers are required to change these;

– Implementing automatic encryption that is state of the art and update when necessary;

– Adding “salt”—random data—to hashed data in order to make it harder for attackers to compromise;

– Using rate limiting, a system for controlling the traffic sent or received by a network, to reduce the risk of automated attacks.

The tension with regard to security is created by the fact that the data of these devices should generally be transmitted very freely in order to most efficiently use the service.\textsuperscript{300} In some instances where the collected data may be sensitive, a two-factor authentication with a password and token seems warranted. Often the main risk for attacks lies in the communication and interaction of various IoT devices, which, if not appropriately secured, present a loophole through which an intruder can hijack the network of IoT devices.

However, first and foremost, no company may put a IoT device on the market that has not been checked for security risks. This request should

\textsuperscript{300} For a general overview see Weber, Internet of things: Privacy issues revisited, 618 et seq.
not only take into account the device but also how customers are likely to use the product, including any surrounding technology which may impact the device’s security.

Once the initial security is set, companies should also focus on maintaining this security level. Regular software updates are commonplace in the IoT setting and enable the addition of new services and capabilities. Security measures should also be updated as well, so as to ensure that the update does not create new security risks that must be addressed before the software is automatically pushed onto the IoT devices. Additionally, the owners of the devices must be informed when the devices are no longer updated and the security thus can no longer be ensured. At this point, the user must decide whether to retain the old device and accept the security risks or buy a new improved device.

The company manufacturing and installing the software on the IoT device should also keep up to date on any identified vulnerabilities that have been identified by other market participants. As IoT device manufacturers rely on other suppliers for parts or software, these vendors may also present a risk. This is due to the fact that the design of their products may also include flaws that may be exploited, and this is why a register of the supplier technology used in the devices should be maintained and regularly checked against national vulnerability databases. The supplier should also maintain a channel, where security researchers or consumers can reach the enterprise about a risk they have discovered in one of its products. Rather than relying on a routine “contact us” link that sends an automated reply, a hotline approach, such as an easy-to-find email box on the website that is monitored regularly, should be considered. Serious inquiries related to the security of a product should generate serious responses.

Bug bounties\(^{301}\) are a good measure to use the available technical know-how of third parties to ensure security by paying a reward to the discoverer of a vulnerability.

---

\(^{301}\) Paying reward for finding loopholes in the system that can be exploited by hackers.
Finally, security should also be understood as a marketing argument, which, if effectively communicated, allows potential customers to feel at ease buying a new and exciting technology even if they do not understand its precise workings.302

III. Labor Law Challenges of IT Sourcing

Not only data protection but also other laws impact the sourcing of IT services. In Germany, for example, a strong focus has been placed on regulating temporary agency work. This affects the common cooperation of external vendor personnel with their service partners. The law only focuses in this context on the factual daily contract implementation. When an employee of the IT company is on temporary assignment at a customer’s enterprise, this enterprise is allowed to direct this employee although he or she is employed by the IT company.

Based on the increased digitalization, ever more IT projects are outsourced and assigned to such contractors. Essentially, these contracts to produce work require the contractor to supply a promised work which requires a certain degree of distinguishability. Such a contract entails warranty rights which the contracting party can rely on if the result does not measure up to the set goals.

Another contract form available is the service contract. This contract has the advantage of only requiring the performance of a certain service and does not owe a result to the contracting party. Thus, warranty rights only apply in a limited fashion. However, the responsibility to carry out and organize the service rests with the service provider, and the employees are generally not bound by the instructions of the customer.

In order to avoid any potential conflicts, the contractor should ensure that its employees are conducting other work than that of the service provider’s employees. Furthermore, a particular difficulty arises in the context of freelancers, which generally are working based on a service contract but in reality receive instructions on a daily basis by the customer.

302 Federal Trade Commission, Building Security in the Internet of Things, 3.
In 2013, the insufficient determination of the assignment models received great attention based on several court cases against large German corporations, including Daimler and Telekom. External contractors were making the claim that they were actual employees of these companies despite having a contract with their employer service company. The market for temporary employees responded rapidly, and companies started to require “to see” licenses for temporary agency work. By asking for the so called “storage licenses,” the companies sought to protect themselves from such cases that may arise based on the lack of a temporary contract or a hidden temporary work agency.303

However, based on a change in law, contractual provisions will no longer suffice to safeguard the contracting business against such claims. In these cases, penalties, social security, and other payments will be sought form the contractors.

A focus of the case law is placed on highlighting the criteria of integration within the work organization and being subject to instructions as a main criterion.304 However, the instruction criterion also presents challenges as contractors will always need some form of instruction to be able to carry out their tasks within a large corporation. In the future, the storage license will come to an end, and every contract of this nature must clearly state that it is temporary agency work. Furthermore, the contractual details of the agreement between the IT service supplier and the customer company must be disclosed to the employee.

However, there are not yet time limits set on these agency contracts. Nevertheless, the contract cannot be for an indefinite period, as this would not qualify as a temporary assignment.305 Currently, a new amendment is being drafted in Germany which would limit such contract periods to 18 months, requiring at least a three-month gap before an employee could be sent to the same customer again. The risk that such an employment contract exceeding the 18 months is invalid will rest on the customer. In such

303 BAG, decision of 12 July 2016, Case No. 9 AZR 352/15.
304 BAG, decision of 30 January 1991, Case No. 7 AZR 51/90.
305 BAG, decision 10 July 2013, Case No. 7 ABR 91/11.
a situation automatically a new employment contract will be in effect between the customer of the agency and the employee which has been sent.\textsuperscript{306}

Importantly, the payment and working conditions must be equal to those employees already working for the customer. From an economical perspective, temporary agency work is only beneficial as the other party bears the burden of a business downturn and the risk of a costly layoff. Importantly, both parties bear penalties when a hidden temporary agency contract is found. Thus, they should seek to include as many characteristics of the contract type they want to agree upon in order to later argue that there is no temporary agency contract.

As a consequence, when contracting a EU agency to supply IT or other staff for a limited duration, any company must closely look to the national law on temporary assignments that can place strong restrictions on such use. Therefore, acquiring specialized freelance consultants and experts is more difficult in the EU than it is in the US, owing to its strong labor protection laws.

\textsuperscript{306} Sec. 9 Nr. 1b & Sec. 10 Nr. 3 AÜG.