

# TIME TO END THE DEBATE: LEVERAGE DATA PROTECTION

---

A change in perspective – statutory requirements  
as a strategic opportunity

**Authors**

Magdalena Buski  
Marc-André Dymala  
Dr Waldemar Grudzien

**Author team**

Christian Böhning  
Johannes von Bonin  
Nadine Hofmann

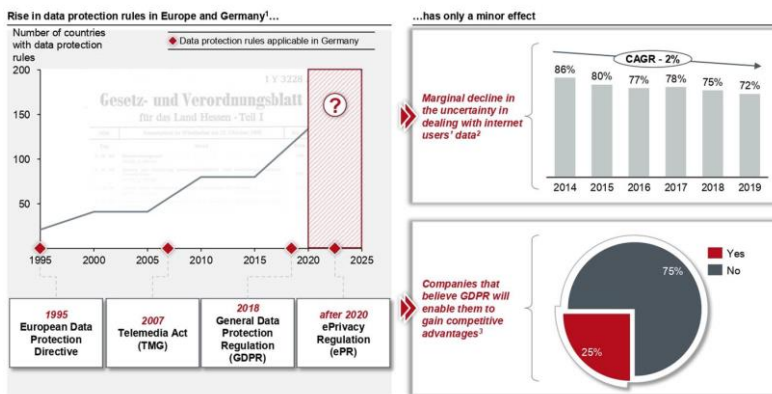
# 1 Introduction

What are the raw materials of the digitised society and, hence, the main factors of production of successful companies in the future? Is it data, which is regularly referred to as the new oil, or rather trust that is the key resource of the 21st century? In actual fact, the answer is both – data and trust in the processing of this data. Confidence that data is processed in line with the will of the data owner and the commercial value of the data – both of which are now reflected in statutory provisions that aim to balance the interests between the participants of the digital economy. The key to gaining this trust is data protection combined with modern information security solutions.

data and trust – raw materials in the digital economy

Regulatory requirements are often perceived as hindering innovation, as a cost driver or even as a necessary evil. This paper is aimed at providing an alternative perspective and encouraging a debate on the opportunities provided by data protection as added economic value. We are convinced that data protection – when used properly – can be a driver of innovation and offers business opportunities.

More stringent regulation does not increase the feeling of security on the part of users and impedes the acceptance of possible competitive advantages



Source: COREresearch (2020) | 1 Der Europäische Datenschutzbeauftragte (2020), Entwicklungsgeschichte der Datenschutz-Grundverordnung | 2 Bitkom (2019), Nutzervertrauen in Datensicherheit im Internet steigt | 3 Der Informationsdienst des Instituts der deutschen Wirtschaft (2020), Datenschutz: Ungeliebtes Regelwerk

Figure 1: More stringent data protection regulation does not increase feeling of security and impedes acceptance of possible competitive advantages

When the EU General Data Protection Regulation (GDPR) came into force in May 2016 and was applied from May 2018 onwards, a comprehensive set of rules was established to protect personal data. This has since been embraced and adapted far beyond the EU in over a 100 countries. In California, which is home to the largest global players in digitisation, as well as for instance in India, data protection laws have been introduced that are comparable to GDPR. In order for the General Data Protection Regulation not to remain a European export that other regions of the world successfully monetise, European companies must act according to their business models and ambitions for data protection. This paper provides guidance in this respect. Chapter 2 clarifies the current situation and shows that the regulations have become increasingly part of corporate reality, and supervisory authorities are also enforcing them more consistently. This is characterised by more intense monitoring

statutory regulations governing data protection in the digital world are being increasingly enforced

---

as well as the strengthening of sanctions in the event that regulations have been violated. Surveys reveal that companies are taking the challenges posed by data protection seriously and intend to implement data protection measures. Nevertheless, there is still a huge gap between aspiration and reality. This is particularly unfortunate since the data that is already available represents a massive economic benefit for companies, but the added economic value is not always used to the extent that is possible due to the fear of violating data protection and the associated penalties. A few – not surprisingly these are the global technology companies – have recognised data protection as a distinguishing feature and are aligning their product features accordingly.

Reflecting on the aforementioned situation, Chapter 3 looks at three main challenges that companies face in terms of data protection and information security:

- › statutory regulations governing the protection of personal data are mandatory and must be implemented in full (as a minimum), since "taking a risk" is ruled out as a result of intense monitoring and the extent of possible (and levied) sanctions
- › many existing business models are currently based on processing personal data, which if not compliant with existing and future – e.g. ePrivacy Regulation – data protection laws are not economically viable or cannot continue unless effective solutions are found
- › new and innovative data-based products and services are either not available on the market or are postponed for as long as data protection compliance cannot be effectively and efficiently ensured. The ensuing economic potential is wasted and market positions are jeopardised unnecessarily.

In order to face the challenges and seize the opportunities provided by data protection, Chapter 4 presents a model for the gradual development of data protection and security. The model describes levels of ambition, beginning with a basic level to ensure minimum legal requirements, through confident handling of extended privacy policies for the active design of trust networks, to the strategic positioning of data protection and data security in the overall strategy as a driver of innovation, growth and competitive potential. The targeted use of IT to achieve data protection efficiently is an inherent part of the step-by-step model and is explained together with presentations of best practice examples, proven tools, checklists and appropriate operational models for setting up data protection management systems combined with information security.

Finally, we summarise our recommendations on making data protection, data and information security proactive. These suggestions may therefore serve to build trust in not only implementing data protection, at a minimum, as a necessary evil, but also to maximise the opportunities and potential of data protection, in order to actively gain and maintain trust – the most valuable resource of the digital economy.

---

business models cannot be implemented without taking data protection sufficiently into account.

---



---

data protection in three steps as an integral part of the strategy

---

## 2 Summary of the status quo

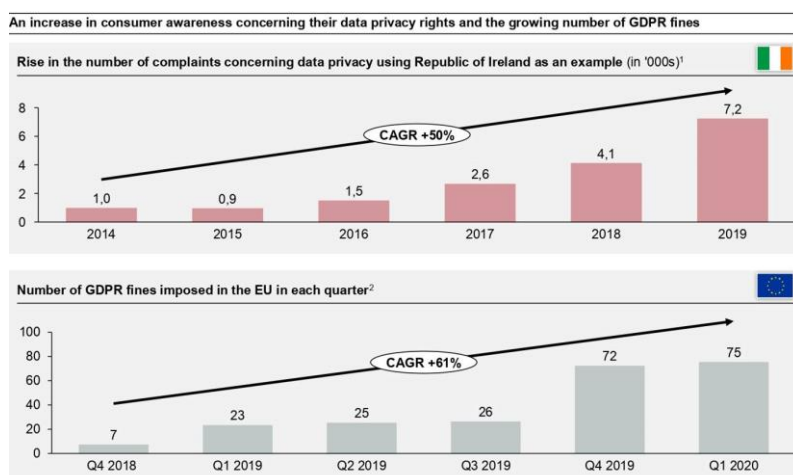
Data protection is still a challenge for companies, even four years after GDPR came into force. Huge fines are the consequences of serious data protection breaches. Despite GDPR having been in force for four years, including two years of mandatory application, initial sanction decisions and increasingly assertive action by the data protection supervisory authorities, most companies are still not fully compliant with GDPR. Dysfunctional strategic and technical implementation, coupled with an over-confidence in one's own data protection capabilities, act as a challenge in an increasingly data-driven market and increase the cost and ever-growing competitive pressure on companies.

### 2.1 Significant fines levied for data protection breaches

Consumers, especially in Germany and Europe, have developed a high level of awareness of data protection in recent years. This awareness is based, not least, on data protection breaches affecting millions of users, such as numerous incidents involving major technology platforms. At the same time, legislators at European level have increasingly focused on data protection. The most prominent example is certainly the GDPR, which came into force in 2016.

international consolidation and differentiation of data protection laws for the digital world

The sovereignty over one's own data is considered an element of the protected individual's development. According to this assessment, individuals are to be protected against any form of disclosure and use of personal data without their consent. Following the strengthening of data protection rights and the consolidation of the legal awareness among consumers/persons concerned, the number of complaints is also rising significantly. (Figure 2). Countries such as Republic of Ireland, often home to the European headquarters of global data processors, show what consequences the awareness of data protection and the self-reporting obligation can have under Article 33 GDPR.



Source: COREresearch (2020) | 1 Irish Data Protection Commission (2020), Annual Report 2019 | 2 CMS (2020), GDPR Enforcement Tracker

Figure 2: An increase in data protection awareness leads to a rise in complaints pertaining to data privacy and the number of fines imposed











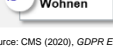

There has been a significant rise in the number of fines imposed across Europe since the introduction of GDPR. Increasing demands on data protection from the regulator, supervisory authorities and customers are exerting pressure on European companies. Since the introduction of GDPR, data protection regulations have been reinforced worldwide. Countries such as the US, China, Japan and Argentina are following suit.<sup>1</sup> California, the seventh largest economic region in the world, is closely aligned with European law with the *California Consumer Privacy Act (CCPA)*.

However, while CCPA was only adopted this year, so that companies have so far been spared from the consequences of data breaches<sup>2</sup>, the 'grace period' for European companies is over. Last year, data protection supervisory authorities took on an increasingly assertive approach. In 2018, average fines amounted to EUR 48,000 per month; in 2019, average fines per month came to EUR 2.9 million, meaning an increase of 5,936% in the first year, excluding ongoing cases.<sup>3</sup>

significant rise in the number of fines imposed in the second year of GDPR being in force (May 2018)

One of the most well-known examples of heavy fines incurred for data breaches is British Airways.

Degree of GDPR penalties imposed by the legislator in several cases (examples)

Company	Country	Date	GDPR infringement	Details of infringement	Fine in EUR m
 British Airways		08/07/2019	Art. 32	User traffic on the website is redirected to a fraudulent website	213
 Marriott		09/07/2019	Art. 32	Data breach: disclosure of personal data concerning 339 million data records	110
 Google		21/01/2019	Art. 4, 5, 6, 11, 13 and 14	Customers are not given sufficient detail on what they can change when setting up a google account	50
 TIM		15/01/2020	Art. 5, 6, 17, 21 and 32	Advertising in spite of lack of consent; incorrect information regarding data processing, deletion periods	28
 Oster. Post AG		23/10/2019	Art. 5 (1), 6	Unauthorised collection and selling-on of 2.2 m data subjects' political affinity	18
 Deutsche Wohnen		30/10/2019	Art. 5, 25	Archiving and ignoring the deletion function, storing without checking whether it is necessary / permissible	15

Source: CMS (2020), GDPR Enforcement Tracker

Figure 3: Evidence of amounts of legal penalties for data protection offences imposed on selected companies

The search term "British Airways data protection scandal" results in over one million results on Google, which can certainly be seen as an indicator of heightened consumer awareness of data privacy rights. The ensuing damage to the company's reputation is immense and is likely to cost as much as the direct fine of EUR 213 million. This example shows just how much uncertainty, inactivity or even non-compliance regarding data privacy can have.

data privacy breaches have a high direct and indirect monetary impact on companies

<sup>1</sup> Accessnow (2019), p 36

<sup>2</sup> Non-payment of fines refers to fines imposed in the US. American companies operating with European personal data or in Europe are subject to GDPR in Europe

<sup>3</sup> CMS (2020), 24.04.2020.

Data protection supervisory authorities across Europe are not shy about imposing heavy fines. The fine may be either EUR 20 million as defined by legislation or up to 4% of global annual turnover recorded in the preceding financial year.

**2.2 Gap between self-assessment and data protection compliance: 70% of businesses are poorly prepared**

The circumstances described above should be seen as a warning to many companies. Analysis and recent project experience show that most companies still do not comply with data protection regulations even though the GDPR has been in force for four years. Even companies that consider themselves to be compliant are, in actual fact, often not compliant due to technical errors. The implementation of GDPR requirements poses challenges for many companies. On an international scale, 42% of companies state that they have difficulties in meeting data security requirements, i.e. technical and organisational measures (TOM) required by GDPR.

over 40% of companies worldwide are overwhelmed with the implementation of data protection requirements

Organisational challenges are reflected in uncertainty about how data protection is handled in the company. This uncertainty is caused by a lack of suitable specialists and training, as well as low budgets in the area of data protection. Similarly, the constantly evolving regulatory framework and the relatively generous scope for interpreting data protection laws currently present a problem. According to surveys, 47% of companies worldwide claim, for instance, that they find it difficult to keep abreast of data protection regulations or fear that they will fall further behind in their already low level of knowledge.

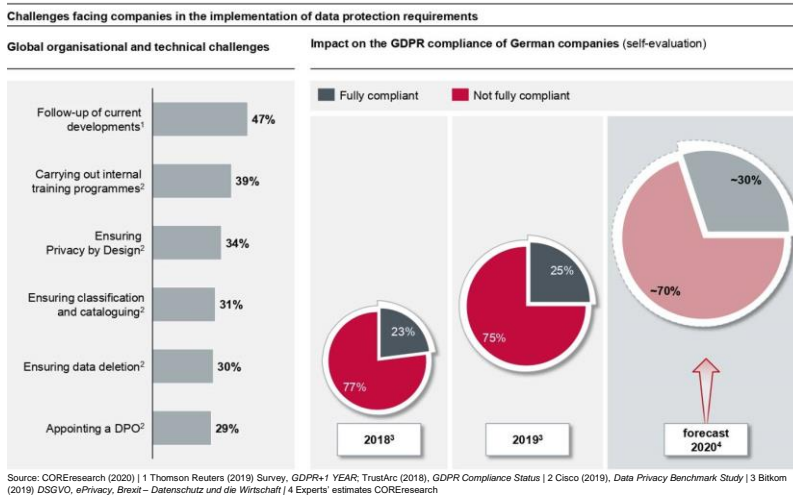


Figure 4: Difficulties in the practical implementation of GDPR result in a high degree of non-compliant companies in Germany

The technical measures required have an even greater influence on the excessive demands made when implementing data protection requirements. 34% of companies face enormous difficulties in complying with the legal "privacy by design". Ensuring the 'right to be forgotten', i.e. erasure of personal data, also represents a major challenge to 30% of

companies. A large number (36%)<sup>4</sup> of companies basically lack an understanding of the tool-supported implementation of GDPR requirements, which cannot be compensated for by means of organisational measures. The excessive demands ultimately result in the small number of GDPR-compliant companies. According to self-assessment, this will be roughly equivalent to a quarter in Germany in 2019 and probably around a third in 2020.

As is so often the case, however, reality is at odds with self-perception. Our project experience has shown that even companies that assume they operate in full compliance with GDPR overlook important aspects:

- › Minimum legal data protection requirements, such as records of processing activities, erasure concept or TOM documentation, are either not available or are of poor quality.
- › Data Protection Officers are appointed but not always notified to the data protection supervisory authority as required.
- › Internal audits on the implementation of data protection-related regulations are not carried out
- › Implementing data subject rights has not been carried out at all or inadequately
- › Cookie management in public websites and mobile apps services is not implemented in accordance with the law
- › Correct deletion of data, after the deadline or when requested, is not guaranteed

The main recurrent cause of aspects that arise is a lack of technical support and inadequate handling of IT solutions to ensure data protection and data security in digital processes.

### 2.3 Growth in the volume of data has great economic potential

Data is increasingly available digitally, and the amount of data processed is rising. By 2025, the global volume of data is projected to increase by 27% annually across all sectors. Not all of this data is personal data within the meaning of the data protection laws such as GDPR, but much is personally accessible or has special economic value in its application vis-à-vis users, consumers, employees, business partners and customers.

Even formerly "analogue" industries, for instance manufacturing or healthcare, can expect an increase in digital personal data. Consequently, material end products and manual work processes are not a guarantee of protection against digitisation. By 2025, 36% more data is forecast for the healthcare sector and 30% more in the manufacturing sector. The "Internet of Things" (IoT) is contributing to a further rise in the volume of data. Applications such as smart home, smart city and smart health are increasingly shifting the economy to the Internet. This is done on a voluntary basis through a strategic decision, or is effectively enforced by GAFAM<sup>5</sup> and BATX<sup>6</sup>. In turn, this development leads to a further increase in data – the "Perpetual Data Machine" has been created.

---

only 25% of German companies rated themselves as being fully compliant with data privacy laws in 2019

---



---

digital availability and data processing are continually on the rise

---

<sup>4</sup> TrustArc (2018), p 10.

<sup>5</sup> Google, Apple, Facebook, Amazon, Microsoft.

<sup>6</sup> Baidu, Alibaba, Tencent, Xiaomi.ppp

## Forecast in the rise of the data-driven economy across various sectors

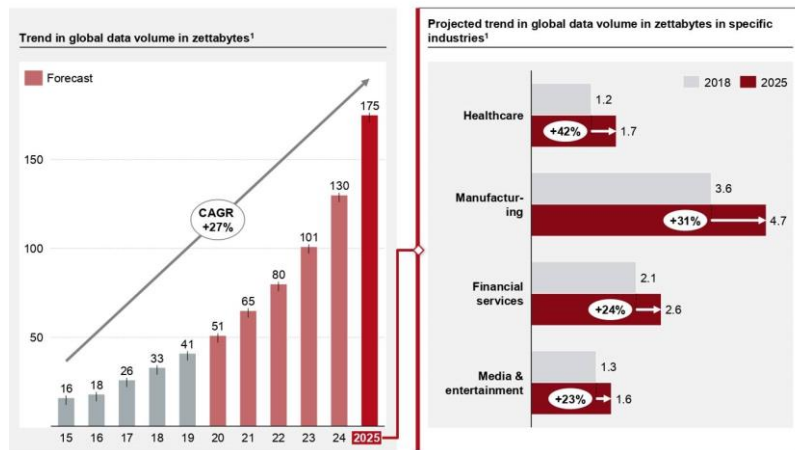


Figure 5: Increasing growth (forecast) of total data volume per sector and worldwide

The volume-based development of the potential of digital data, promising possibilities of utilising data as a result of new technologies such as artificial intelligence (AI) and the development of new business fields are on one side of the "data coin". An increase in data is usually synonymous with an increase in personal data. This development causes an explosion in costs for companies that carry out data protection-relevant processes manually because the cost and time involved in manual processing potentially rises with an increasing amount of data. This situation, as described in the previous chapter, affects most companies, meaning that the resulting flood of data thereby generated is often at odds with the protection of data privacy. Principles governing GDPR, such as data minimisation or storage limitation within the meaning of Article 5(1) c), e) GDPR, can only be guaranteed with difficulty.

Besides self-induced errors, data maximisation may also lead to indirect errors caused by third-party processing. For example, the volume of data produced and used creates the need for high storage capacity that is not economically viable for companies to provide themselves. Outsourced backups, archives as well as the destruction of data media have long been typical processing activities carried out under contract. These are now supplemented by Internet-based or cloud-based storage facilities provided by third parties. These processors can be, for example, data warehouse services that enable big data analysis. Furthermore, multiple tool environments operating in the cloud process personal data using developer, marketing and analysis tools, and then pass it on to processors. The party issuing the processing order may be completely unaware of which tool processes its customers' data without its consent.

increasing data volumes have business potential if data privacy is efficiently implemented



---

The problem is that although the data comes under the control of these third-party providers, the responsibility for it is retained by the controller. The processor acts on behalf of the controller, who must ensure, in accordance with Article 28(1) and recital 81 GDPR, that the processor "provides sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including those relating to security of processing". In the event of incorrect data processing on the part of the processor, the controller and the processor are jointly and severally liable for the processing in accordance with Article 82 (4) GDPR.

Besides being liable, offences committed by contracted processors have additional implications on the controller's reputation. It is not the processor but the controller who has to disclose data breaches that are likely to pose a high risk to personal rights and freedoms. They must notify both the data protection supervisory authority in accordance with Article 33 GDPR and the data subjects in accordance with Article 34.

Consequently, generating ever-more data increases the overwhelming demands on companies to implement data protection requirements. The risks and consequences of both internal and external data processing must be assessed by means of a data protection impact assessment and dealt with using adequate technical and organisational measures. To this end, data flows and data sources must be known and the expertise for the technical and professional implementation of data protection must exist. Often, companies cannot guarantee these prerequisites. This provides a possible explanation for why the necessary investments in data protection have not (adequately) been made or why the risk of fines for data breaches resulting from lack of compliance due to excessive manual implementation costs is not being taken into account.

---

data processing is increasingly outsourced – companies are liable for errors by external third parties

---

---

positive data generation generally has a reinforcing effect on the excessive demands placed by data protection

---

### 3 Doing business without data protection is virtually impossible

Supervisory authorities are increasingly putting pressure on companies. They impose stricter measures, widen controls and fines to an increasing number of sectors and companies. At the same time, new regulatory data protection requirements are already in the legislative process, since the ePrivacy Regulation (ePR) will further increase regulatory pressure. As a result of the ongoing development of the legislation, the evolution of the companies is being hampered. However, this is not due to the regulations themselves, but to incorrect strategic assessment of the value of data protection and fear of data protection breaches by companies.

#### 3.1 Risk acceptance is no longer an option

While established companies were initially subject to heavy fines, data protection supervisory authorities are now increasingly focusing on smaller companies, including private individuals.

Fines have been imposed totalling approximately EUR 25 million since the introduction of GDPR in Germany. Nowadays, the average amount per data protection breach is around EUR 1 million, compared to around EUR 9,100 in 2018.<sup>7</sup> The supervisory authority is taking full advantage of its supervisory remit across all sectors:

supervisory regimes are being tightened up - supervisory authorities are increasingly exploiting the full range of penalties

Sector	Company/institute	Description of breach	Fine in EUR '000s
Real estate	Deutsche Wohnen SE	Non-compliant archiving (Art. 25 GDPR)	14,500
Telecommunications	1&1 Telecom GmbH	Unlawful disclosure of personal data / inadequate technical and organisational measures (infringement of Art. 32 GDPR)	9,550
Delivery services	Delivery Hero Germany GmbH	Storage of data without any legal basis / disregarding the right to erasure (Art. 15/ 17/ 21 GDPR)	195
Healthcare	Hospital in federal state of Rhineland-Palatinate	Publication of healthcare data / inadequate technical and organisational measures (Art. 32 GDPR)	80
Finance industry	N26	Storage of personal data without obtaining consent from data subjects (Art. 6 GDPR)	50
Transport services	Hamburger Verkehrsverbund GmbH	Failure to report security gaps on the website despite customers drawing attention to them (Art. 33/ 34 GDPR)	20
Social networks	Knuddels.de	Personal data exposed as a result of a cyberattack (Art. 32 GDPR)	20
Food and beverage industry	Restaurant in Saarland	Unlawful video surveillance of customers (Art. 5 GDPR)	2
Public service	Police officer	Personal data acquired unlawfully during the course of duty (Art. 6 GDPR)	1.4
Private individuals	Citizen	Publication of recordings of public road traffic on YouTube without obtaining consent from those concerned (Art. 5 GDPR)	0.2

Source: CMS (2020), GDPR Enforcement Tracker

Figure 6: Heavy penalties pertaining to data privacy breaches levied on companies across different sectors in 2018–2019

The end of last year already saw data protection-related sanctions increasingly geared towards small businesses and more minor breaches. For example, a police officer was fined EUR 1,400 for illegally obtaining personal data (Figure 6).

hiding behind large corporations is a thing of the past – focus on the broader economy

<sup>7</sup> CMS (2020), 03.05.2020.

The increasing volume and value of fines speak for themselves. More and more companies can expect to be faced with checks by the supervisory authorities in the future and will have to come to terms with the consequences of an audit. This assumption is confirmed by two additional factors: there is a disproportionate rise in the number of fines imposed each month. Furthermore, staffing at data protection supervisory authorities has increased across Europe in 2019 (a rise of up to 30% compared with the previous year) and budget resources have also risen (by up to 70% on the previous year). Germany witnessed a budget rise of 28% in 2019 and a 3% increase in staff, based on information provided from only 7 German states and the federal authority. Consequently, acceptance of risk will no longer be an option in the future, as companies will no longer be able to remain hidden in the shadows of the corporates.

disproportionate increase in supervisory authorities in terms of staff and budget

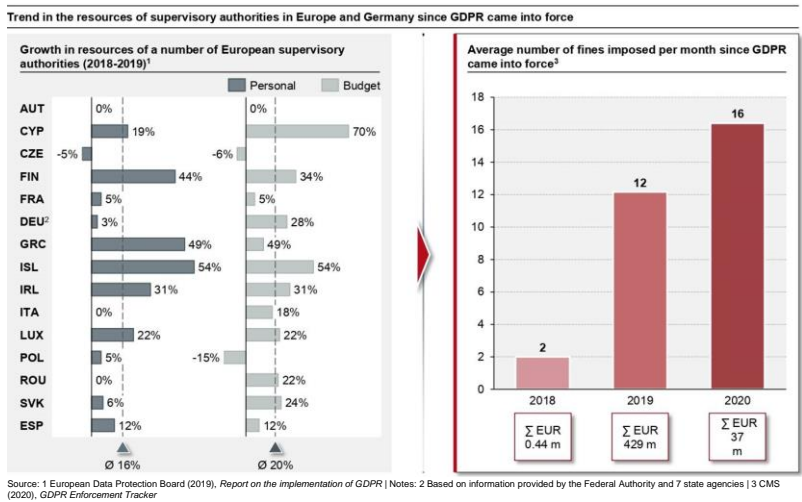


Figure 7: Reinforcing the resources of the supervisory authorities is resulting in a rise in the average monthly penalties levied pertaining to GDPR

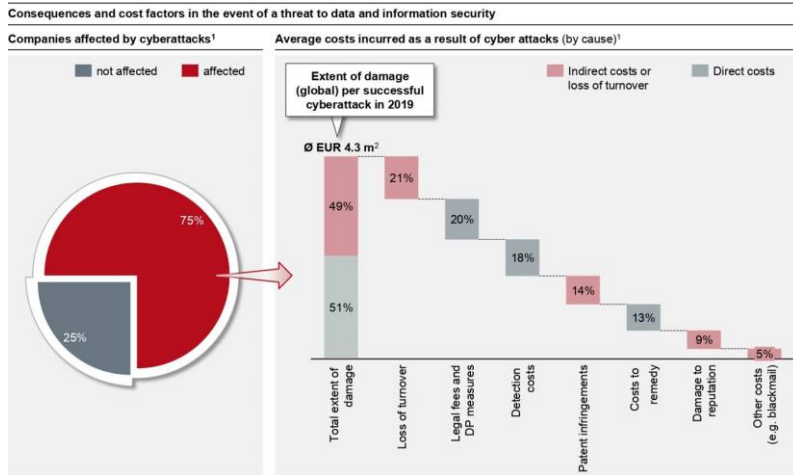
Concentrating on supervisory authorities, whilst very important, is not the only perspective required. Indeed, the huge costs of data protection law are a mere fraction of the entire costs of a data breach. By way of an example, the average total cost amounts to EUR 4.32 million per incident for a data protection infringement. Data breaches and cyberattacks mainly disclose credit card data, app users' data, passwords and personal data, including photos<sup>8</sup>, which make them data protection incidents. Back in 2019 alone, 75% of German companies were affected by cyberattacks. Incidents which are as a result of inadequate technical and organisational measures within the meaning of Article 32 GDPR, are subject to heavy fines. Nevertheless, only 20% of total cost comes from sanctions.

data protection incidents are often the result of information security incidents

<sup>8</sup> Handelsblatt (2019), p16.

Total costs comprise several direct and indirect elements. Direct costs stem from the costs involved in detecting the incident in the first place: Companies require, on average, 69 days<sup>9</sup>, to find and rectify data leaks – 69 days involving disruption as systems initially have to go offline – 69 days where automated processes have to be carried out manually, meaning that there is a significant drop in productivity and income, if not a total loss – 69 days that account for 18% of the total costs attributable to a data leak. In terms of indirect costs, damage caused to the reputation – at 9% – is yet another data protection-relevant cost factor attributable to cyberattacks.

30% of total costs of a threat to data security are due to loss of turnover (21%) and damage to reputation (9%), which also have an additional impact



Source: <sup>1</sup> Bitkom (2019), *Angriffsziel deutsche Wirtschaft; mehr als 100 Milliarden Euro Schaden pro Jahr*; percentages derived from cyberattack costs in the past two years | <sup>2</sup> Geldinstitute (2020), *Millionenschäden: Die Kosten eines Datenlecks*

Figure 8: A threat to data and information security results in far-reaching indirect and direct costs

Damage to reputation thus continues to unfold long after the actual event, as users will become increasingly sensitive, and media coverage will result in negative headlines reaching a wide audience, creating privacy concerns to both existing and new customers.

### 3.1 Existing business models under pressure – need to adapt to data protection laws

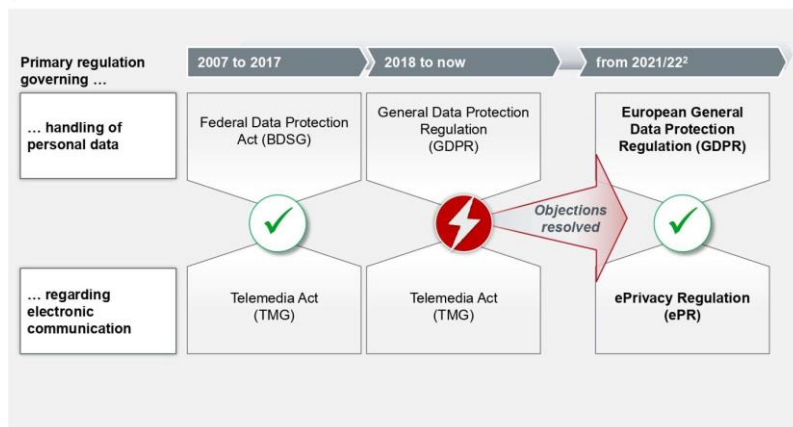
In the data-driven market, cookies, tracking, consent and profiling are well-known keywords that companies already use in their marketing. At the same time, keywords are also very much the focus of discussions on data protection between respondents, supervisors, consumer protection organisations and the business community, as the legal form of their use in online marketing is unclear. At the heart of the debate is the question of the legal basis on which user data (user data and usage data) may be used by the First Party and transferred to the Third Party (advertising networks, Google, Facebook, etc.). Does the intentional processing of personal data for tracking, advertising and user profiling – summarised as “data services” – require the consent of the user?

legislation is unclear concerning the handling of cookies, tracking, consent and profiling – the ePrivacy Regulation (ePR) and amendment to the German Telemedia Act (TMG) attempt to remedy this

<sup>9</sup> Die Welt (2018), 18.05.2020.

To date, economic entities have been unable to reach an agreement on one issue: data protection supervision requires consent under Article 6 (1a) GDPR. The online advertising industry, such as media companies, refers to Section 15 (3) of the German Telemedia Act (TMG), under which the needs-based composition of telemedia allows the use of pseudonymous usage profiles with objection (opt-out) or, in accordance with Article 6 (1) f) GDPR, whereby the legitimate interest of the media company must be regarded as more important than that of the user not to use their data in question for data services. This ambiguity continues to leave room for interpretation of the law which, for example, website operators actively exploit to increase the conversion rate for pseudonymous user tracking. The ePR and the amendment to TMG are intended to remedy this debate and clarify the GDPR in the area of electronic communications:

Different directions of GDPR and TMG – ePR to “tip the scales”<sup>11</sup>



Source: COREresearch (2020) | 1 Regulation (EU) 2016/679 (General Data Protection Regulation) latest version according to the worksheet L 119, 04.05.2016 | Federal Ministry of Justice and Consumer Protection (2007), Telemedia Act, dated 26 February 2007 (BGBl. I p. 179), last amended by Article 11 of the Act from 11 July 2019 (BGBl. I p. 1066) | 3 European Commission (2017), Vorschlag für eine Verordnung des europäischen Parlaments und des Rates | 2 Voraussichtliches Inkrafttreten

Figure 9: Conflicts in data privacy laws to be resolved by adopting ePR

According to Article 5 (3) of the ePR draft, informed consent based on clear and comprehensive information regarding the purposes of processing is absolutely necessary. If the TMG follows the draft ePR, an opt-in will be codified for all tags relevant to data service<sup>10</sup>. The consent itself will then have to comply with the provisions governing Article 7 GDPR, such as the verifiability of the consent granted.

besides current regulations, provisions must be made for future additive requirements under ePR.

In its judgement (067/2020 dated 28.05.2020) concerning consent given to telephone advertising and cookie storage, the German Federal Court of Justice ruled that consent must be obtained from users, at least for cookies used to profile users for advertising and market research purposes and to make telemedia suitable for use. A banner is no longer sufficient. The problem is that the adoption of ePR has been pending for more than two years and the ultimate legal form can only be assumed. Nevertheless, the outcome will have an impact on both technology and, in particular, on companies' business models. The main focus of current debate is primarily the impact on technology. In the case of personalised or pseudonymous identification tags, there will, of course, be new techniques for identifying users, assigning the redirect chain and targeting as the final step before advertisements are actually delivered. But this is ultimately obsolete, as techniques in future will all be considered, in legal terms, as “invasive tracking”, without the user's consent, and solutions in the form of e.g. consent management platforms are already being identified and established. Instead, the debate should shift towards the uncertain implications on companies' business models. After all, what does this mean for the business models of the online advertising industry, such as media companies?

<sup>10</sup> Tags are 1st, 2nd and 3rd cookies, JavaScript ID as session cookies, evercookies, customer ID, device/behavioural fingerprinting, ID consortia, etc.

---

In this context, there is uncertainty for both companies and regulators. The Bavarian State Office for Data Protection Supervision is pro-business: If the aims of the GDPR prevail, the interests of those responsible must also be recognised, which would mean, by implication, that the user would not have the right to use a website freely and free of charge. On the other hand, the supervisory authority of Baden-Württemberg takes the view that the provision of a service cannot be linked to the processing of data<sup>11</sup>. This is interesting with regard to the opinion of the European Article 29 Working Group on news media<sup>12</sup>: "There is a clear democratic need to ensure the economic survival of the news media. However, the European Commission should not accept that news media forcefully introduce invasive tracking of users." Consequently, news media should survive, but not with tracking. It goes without saying that a print medium is paid for at the kiosk, but the audience presumes free use in cyberspace.

---

the focus on solving technical issues is not sufficient for future ePR regulations.

---

In the long term, there are far more powerful opponents of the online advertising industry and of European regulation and supervision: browser (developers). All common browsers now block third-party cookies and sometimes even first-party cookies. European policy is entrusting an increasing number of privacy functionality to browser developers (essentially GAFAM in the European market). Can a business still serve its users and customers by means of a consent management platform, or is this control taken from the user's browser? The access barrier is moved by the content producers to the browsers as gatekeepers. If advertising can or cannot be played with the presence of consent, the content itself can also be controlled. Is this a desirable approach for the European economy as a whole? Does this not undermine the sovereignty of independent and freely acting commercial enterprises and, ultimately, of Europe?

But one key question must, above all, be asked: How long can a business model be successful against the will of the users? Or is the economy not more successful with an informed client who can decide whether or not to give consent? Data services with consent are better than data services without consent as they are more accurate. At the same time, fear of monitoring has the same effect as actual monitoring. The user should therefore be persuaded by good content, useful services, etc. to give consent. The effect of users' constant self-improvement (cf. Wollen → Können<sup>13</sup>) cannot be ignored and so must be accepted. Products and services must be structured accordingly and made available to the user. Appropriate solutions are required to make the value of the user data transparent and to enable an informed, autonomous decision to consent to the use of the data by the data owner.

---

a business model with user's consent is more promising than one without

---

The amount of questions and possible answers is symbolic of the uncertainty of companies. It is apparent that a secure approach to data protection is becoming increasingly important, as any further development of data protection law increases the complexity around data protection and calls for technical implementation and, where appropriate, adaptation of its own business model.

---

<sup>11</sup> Bundesverband Deutscher Zeitungsverleger e.V., (2019), 05.12.2019.

<sup>12</sup> European Commission (2016).

<sup>13</sup> COREresearch (2015), Whitepaper: Wollen → Können (is equivalent to willingness and ability).

---

**Aside: possible idea for the use of data through media companies (also feasible for scenarios in other industries) in the context of the ePR – business models**

The categories could be subdivided into Basic, Eco, Comfort and Premium.

- *Basic:* The content freely accessible content to the user consists of a basic service (derived from the service mandate of ARD and ZDF)
- *Eco, Comfort and Premium:* Here, the basic service is supplemented by additional content, which can be configured as desired depending on which offer category (Eco, Comfort, or Premium) is chosen. The basic idea is that additional content must be paid for, either by means of money or in data.

The basic service content can be supplied by the provider completely free of charge and free of data, or paid for by means of pseudonymous first-party tracking (suitable advertising based on consumed contributions). Further content is paid for by pseudonymous first- and third-party tracking. Such payment using data can also be dispersed across the entire service offer. Monetised customers do not pay for data services unless, for example, they want personalised advertising from their newspaper (first party) and/or from selected advertising partners (third party) of the



### 3.3 Waste of the potential for digitalisation for fear of fines and strategic misjudgement of data protection

The multiple challenges described in the previous chapter as a result of a lack of knowledge on data protection and the major uncertainty of further undecided legal developments and of data protection supervisory authorities lead to the “Data protection powerlessness” of companies.

All in all, this means companies fail to vigorously drive forward the necessary (digital) developments or even refrain from doing any:

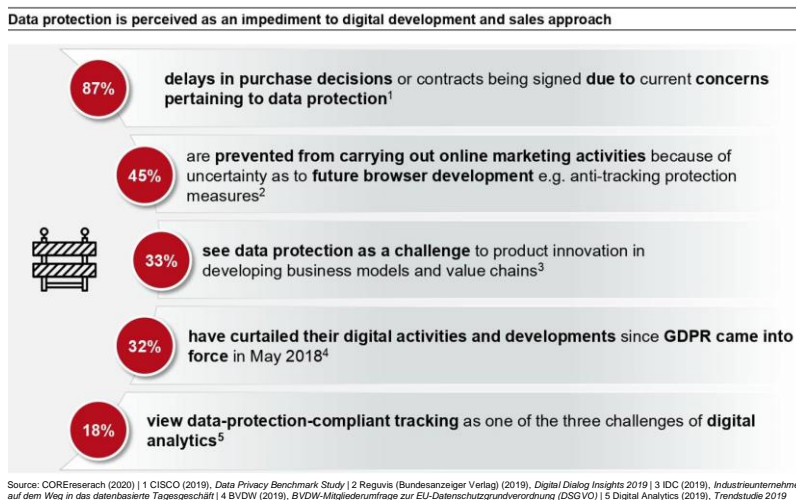


Figure 10: A lack of data protection know-how hampers innovation and digital development

Whether it be online customer acquisition, the use of new technologies such as artificial intelligence for analysing customer behaviour, or the use of clouds to efficiently automate processes and save costs – Innovation is hampered by a company's concerns regarding data protection, meaning that product innovations are, therefore, either delayed or do not happen at all. As a result, organisations fail to master the regulatory requirements and thus are hampering further development, which is indispensable for the company's success. The digital and increasingly data-based development of the market cannot be halted. Conversely, dealing with and investing in data protection are essential.

We can establish that a basic problem lies in the strategic misjudgement of data protection by companies. Two contrasting developments can currently be observed: On the one hand, customers' awareness of data protection is increasing. 78% of users are concerned about the safety of their online data<sup>14</sup> – “Customers no longer buy brands that offer good products, they buy from brands they trust,” said the English author and Oxford lecturer Rachel Botsman<sup>15</sup>.

necessary product innovations and ongoing development of the business model is abandoned due to data protection concerns

<sup>14</sup> Ipsos (2019), p 8.

<sup>15</sup> FAZ (2019), 03.05.2020.



---

On the other hand, a large proportion of companies have not understood the significance of data protection for their customers and, subsequently, for their own success. This is because 63% of the 862 German companies interviewed do not see GDPR as an opportunity and a competitive advantage<sup>16</sup>, although it aims to safeguard the data protection rights required by customers. 47% even consider GDPR to be anti-competitive<sup>17</sup> instead of using it as a framework for regaining customer confidence and actually recognising the enormous role data protection now plays for customers and other stakeholders.

These relationships of customer trust, acceptance and data protection appear to be better understood and embedded in successful technology groups such as Apple and Facebook. This is because they have changed their mindsets – they are increasingly advertising with privacy-friendly settings and product features, e.g. Apple: “Privacy. That’s iPhone.”<sup>18</sup>. They are making a statement, thereby satisfying (at least perceived) customers’ need for data privacy and are establishing themselves as a trustworthy supplier; they are thus favoured by customers.

---

the majority of companies are strategically wrong about data protection – a few develop competitive advantages from adopting a strategic approach to data protection

---

---

<sup>16</sup> IWD (2020),01.05.2020.

<sup>17</sup> IWD (2020),01.05.2020.

<sup>18</sup> YouTube (2019) Werbevideo von Apple, 03.05.2020.

## 4 How to gain sovereign competition with data protection

It is possible to follow the method used by most companies and see data protection as a necessary evil, bureaucracy monster and object of revision, or to take a different approach and use data protection as an anchor of trust for customers, a differentiator in competition and thus as a further (equal) basis for the design of a sustainable successful business model.

This approach has been recognised by some companies that see a number of benefits in complying with data protection:

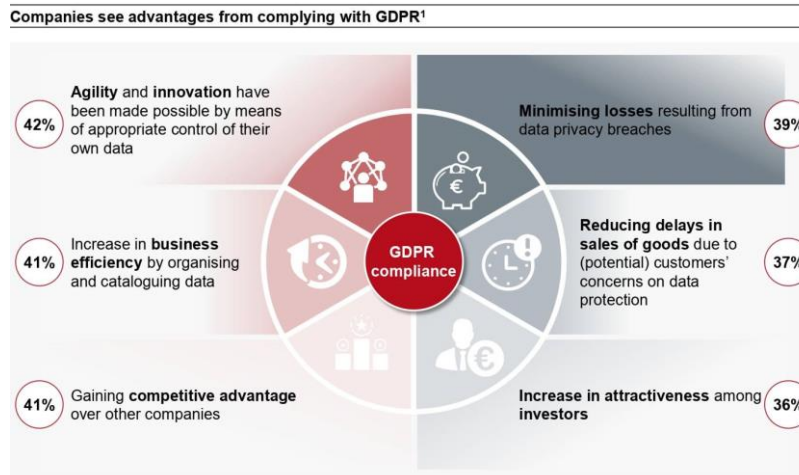


Figure 11: A selection of companies perceive benefits from data protection compliance

Focusing on the opportunities that data protection offers, we first set out a three-stage approach that will enable a company both to comply with GDPR and to generate competitive benefits through trust-building data protection.

Modern data protection requires technologically-designed data security. Of course, data protection and data security can also be implemented manually, but not on the basis of competitive characteristics and at a competitive cost. In this respect, we highlight the benefits of modern IT architectures, including that used for data protection. In the final part of this chapter we use the experience of our transformation practice to, on the one hand, explain facts in a concise manner and, on the other hand, to give recommendations for implementation.

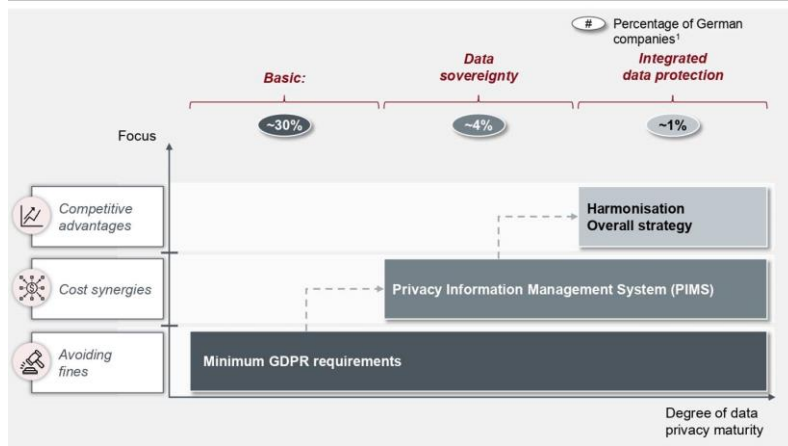
### 4.1 3-step model – compliance, sovereignty, integrity

The level of ambition in meeting data protection requirements may vary according to an organisation's objectives. Whereas some companies state they simply wish to achieve mere compliance with data protection rules, others will want to add value through data and data protection. With this in mind, we have developed an approach that includes three levels of ambition. The 3-step model has been broken down, starting with basic, and this level complies with the law for all business activities. In the second level, the company acquires sovereignty over data protection. In the third level, the data protection strategy is an integral part of the overall strategy,

companies that view data protection as a strategic element see various competitive advantages

and thus allows data protection to be offered as a product and service on the market.

Transformation in 3 steps to integrate data privacy into corporate strategy



Source: COREresearch (2020) | 1 Experts' estimate COREresearch (2020)

Figure 12: The 3-step data privacy model serves as an aid for sustainable integration of data protection into corporate strategy

- The first stage, 'Basic', is intended to provide compliance with GDPR, i.e. compliance with the law. By completing this stage, sanctions due to data protection breaches can be efficiently avoided.
- The end product of the second stage is a privacy information management system (PIMS) and thus the generation of income from data through the appropriate handling of it. Furthermore, the company also obtains the ability to certify data protection.
- During the final stage, data protection becomes an integral part of the overall strategy, thus achieving competitive advantage, synergies and mastering the future of data-driven business models are achieved.

---

3-step model for the individual development of data protection in the company

---

Depending on the degree of data protection maturity, different starting points are appropriate. It must be stressed here that all three stages build on another. For example, the benefits of the third stage can only be attained by passing through the first and second stage.

### 4.1.1 Basic – result: compliance

Achieving a 'Basic' level means that the personal data processed enables the company to ensure the necessary legal compliance. In this respect, the GDPR mentions ten key points:

the basis for this is to ensure that minimum legal requirements are effectively met.

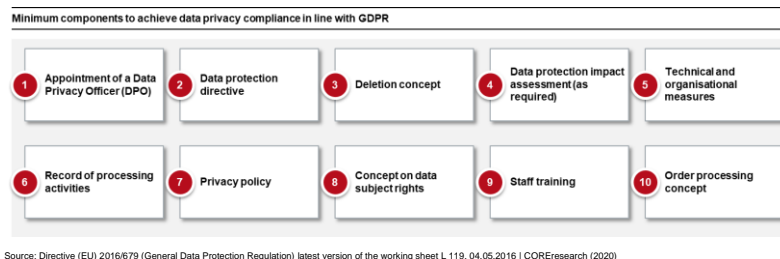


Figure 13: Minimum components of data privacy compliance and list of processing activities in line with GDPR

As part of the monitoring function, a Data Protection Officer (DPO) must be appointed and notified to the data protection authority responsible for the federal state in question. The latter is not subject to carrying out instructions on data protection issues and is responsible for meeting all tasks set out in Article 39 GDPR. In practice, these include, among others, creating a data protection policy, a list of processing activities and an erasure concept, which comprises, inter alia, the provision of a list regarding all activities with a retention period or a deletion period and provide information on the handling of backups and archives. The DPO is also responsible for checking the requirement and, if necessary, carrying out a data protection impact assessment, ensuring technical and organisational measures and ensuring data subjects' rights are respected. They are also responsible for defining and implementing a concerted approach to dealing with data subjects' rights, which is part of comprehensive training for all staff. Finally, the need for and possible implementation of outsourced processing must be checked as part of the framework of a standardised procedure.

---

In most instances, Basic will have to be applied ex post, in order to achieve compliance with the law in the first instance and thus to avoid sanctions for data breaches. Basic may also be applied from the outset, for which, however, a management system is inevitable. Basic also lays the foundations for the second stage of the PIMS in addition to data protection compliance.

Of the 10 key points, we have detailed four absolutely mandatory documents below, based on our expertise and practical experience. These documents are well defined in regulatory theory but introduce a number of obstacles in their implementation.

The four documents are

- › Records of processing activities
- › Erasure concept
- › TOM document
- › Appraisal of the need to carry out a data protection impact assessment

*The record of processing activities manages the documentation required as well as fulfilling the reporting duties of GDPR*

In the event of a data protection audit, the supervisory authority will give a week's notice before undertaking the audit and, secondly, request immediate inspection of the directory of processing activities. It is not of ultimate priority that the directory of processing activities fully coincides with the data protection reality. It is much more important to be able to provide a plausible list of processing activities which is up to date and shows that the controller implements data protection in practice in a methodical, comprehensive and literally responsible manner. A good list of processing activities lays the foundation for the remaining documents, most especially for the erasure concept and for the technical and organisational security measures.

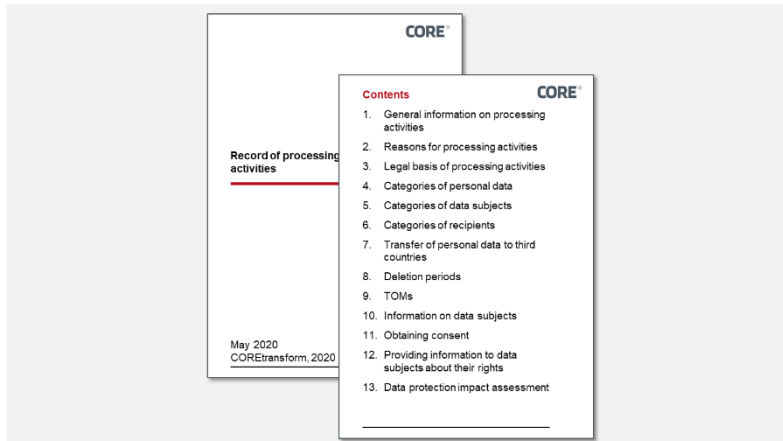
---

no need to be afraid of the list of processing activities

---

What is more, an excellent list of processing activities not only documents the minimum content required by Article 30 GDPR, but also all the obligations from the other articles, in order to be able to account for the legal basis of the processing operations such as envisaged storage limit and data subject rights. Consequently, the list of questions concerning a processing activity not only comprises the cover sheet and at least 8 questions but 13 questions:

Template of the record of processing activities



Source: Directive (EU) 2016/679 (General Data Protection Regulation) latest version of the working sheet L 119, 04.05.2016 | COREresearch (2020)

Figure 14: Structure of the record of processing activities

*Control over deletion is restored by splitting the erasure concept into organisation and application*

From experience, we recommend that data-driven companies subdivide their deletion concept into organisation and application. Organisation takes on the role of the operator of the application. In the organisation, sanctions imposed due to data protection breaches are avoided, in the application benefits are generated by data protection. The benchmark for all deletion concepts is DIN 66398 (“Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information”). The erasure concept is described in the following steps:

- › Specifying data types
- › Specifying standard deletion periods Identifying the starting times
- › Setting the deletion classes Implementing deletion procedures

As far as the organisation is concerned, we would recommend drawing up a table containing essential laws on duration of data retention and when it has to be deleted, such as Section 147 German Fiscal Code (AO), Section 257 German Commercial Code (HGB), Sections 195 and 199 German Civil Code (BGB), Article 6 and Article 17 GDPR and Section 26 Federal Data Protection Act (BDSG) regarding deletion periods and the starting periods derived from them. The deletion class table can then be set up in line with DIN 66398 for the application and its mainly few processed personal data types.

*Technical and organisational measures (TOM) can be counted and automated*

The TOM document describes all measures taken to ensure the security of the processing of personal data. In accordance with Article 32 GDPR, the data controller and data processor shall implement appropriate technical and organisational measures to ensure that personal data is protected. The Regulation states the following measures:

- › The pseudonymisation and encryption of personal data,
- › The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services in conjunction with the long-term processing
- › The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- › A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

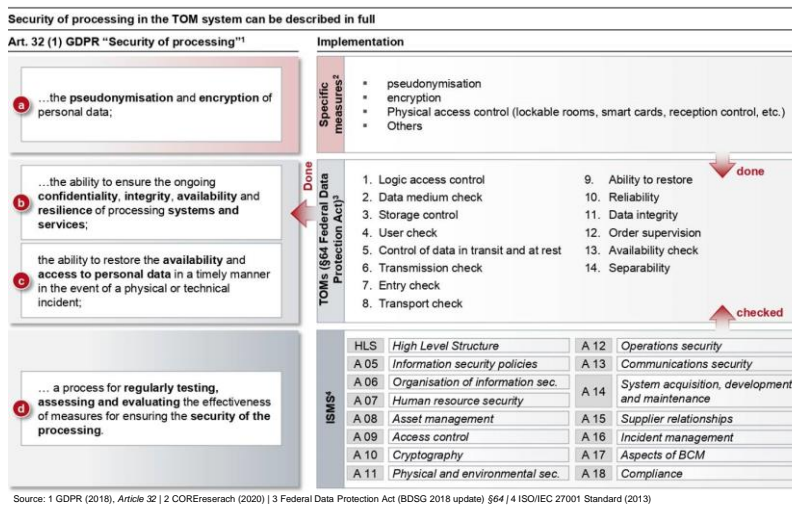


Figure 15: To achieve security in data processing, it is necessary to establish a TOM system in the company

Consequently, Article 32 GDPR, in conjunction with Section 64 of the Federal Data Protection Act (BDSG), contains all the components to prepare a TOM system. These components consist of 14 technical and organisational measures which can actually be implemented using specific measures. There are only a set number of combination options for TOM and specific measures, meaning that the TOM system can be fully described and automated. Even the fourth requirement in Article 32 GDPR – “a process for regularly testing, assessing and evaluating the effectiveness of TOM ...“ is already in place for a well organised controller in the shape of an Information Security Management System (ISMS). As a result, a TOM system can be set up as shown in Figure 15 and can be used as proof that specific measures have been introduced as well as for setting up contracts when processing activities are outsourced.

best practices provide suitable templates for an automated TOM system

*The need for a Data Protection Impact Assessment can be initially checked using a catalogue*

A Data Protection Impact Assessment (DPIA) must be carried out if the anticipated processing is likely to result in a high risk to the rights and freedoms of individuals. In this respect, the controller must carry out a prior assessment of the impact of the envisaged processing activities in terms of protecting personal data. The legislator and supervisory authorities offer four methods that can be developed into a structured approach for DPIA preliminary examination. The first method is the “classic” method of risk management: a matrix of probabilities and potential extent of damage. Then there are

- Three abstract cases from Article 35 (3) GDPR
- “2 of the 9 criteria” - method of Article 29 working party stating nine abstract processing transactions
- An explicit list of processing activities from the Data Protection Conference identifying 17 specific processing operations

In theory, it is sufficient to check the requirement of a DPIA using only one method. But in reality it is more complicated: We would not recommend using the matrix method and instead to check using the three remaining methods. If all three methods result in a “no”, then a complete DPIA is not necessary.

DPIA should only be applied where it is really required, large-scale avoidance is possible

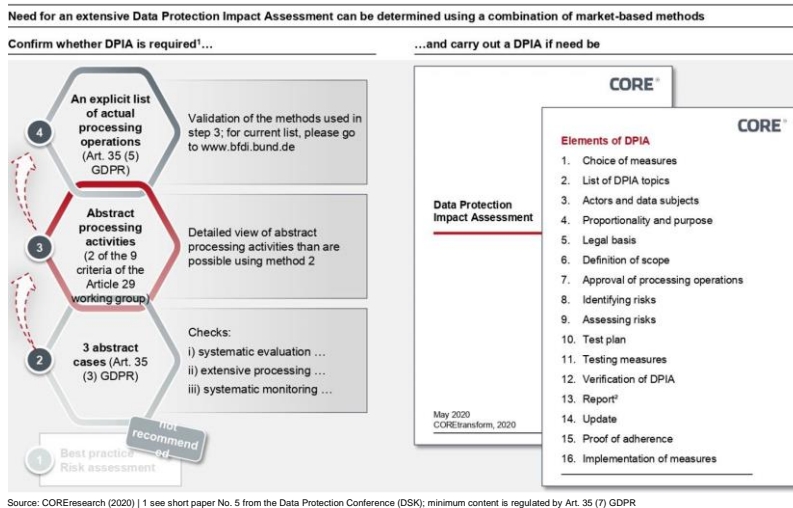


Figure 16: Verification by means of a Data Protection Impact Assessment can be carried out in a methodically structured manner

#### 4.1.2 Data sovereignty using a Privacy Information Management System

Whereas the first step focuses primarily on achieving external GDPR compliance, the second step aims to build long-term compliance from within. The necessary modules are laid as a basis during the first step, but in most cases they are not yet apparent in the company.

A system that harmonises individual measures and specific data processes, and actually implements policies will be necessary.

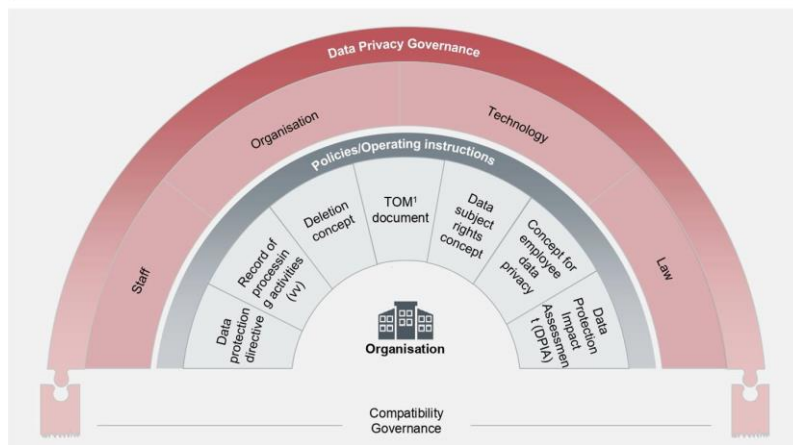


The Privacy Information Management System (PIMS) defines the tools and methods by which the management of an institution can control the tasks and activities aimed at data protection in a transparent manner. Consequently, a PIMS assists in defining, managing, checking, maintaining and continually improving its own level of ambition in data protection. Only once a PIMS is introduced, can data protection compliance actually be implemented sustainably through an in-house organisation.

the Privacy Information Management System harmonises the whole of all data protection processes and concerns of a company

By creating a PIMS, data protection is considered to be a closed (management) system, making it easier to connect to other management systems such as information security management system and its associated strategy. Specific elements such as “Basic” data protection components can now be combined in a targeted, forced manner across various management systems as a result of the higher level of control.

Recommended structure and compatibility of a Privacy Information Management System (PIMS)



Source: COREsearch (2020) | 1: Technical and organisational measures

Figure 17: The set-up of a Data Protection Governance is a prerequisite for creating a compatible Privacy Information Management System

The overall control described above is achieved by extending the minimum data protection of the “Basic” level in all dimensions through the establishment of data protection governance. This comprises four overarching levels: Personnel (list of staff), organisation (set up and workflow), technology including technical measures and law (legal perspective).

PIMS reveals its effect on four levels: staff, organisation, technology and law

In this respect, it is important that no level can exist by itself. They can only develop to their full effect when in unison. That is the reason why we recommend setting up the levels gradually and in parallel if they are not already in place. Consequently, the order of the four levels do not, in any way, imply priority. We are fully aware that the desired level of ambition cannot be achieved overnight, which is why selected elements of the PIMS are introduced as part of the statement, which are key to the set-up and, of course, can and have to be adapted and supplemented individually to the company concerned.

---

## Staff

The most important staffing appointment in respect of data protection is the Data Privacy Officer (DPO). Whether or not the appointment is internal or external is only important as far as notice periods and liability are concerned. The position is generally recognised and filled in most companies, although not actively deployed. The DPO is usually involved too late in the decision-making process, or not at all. As many companies do not realise the importance of involving the DPO in the decision-making process, or even face difficulties in including them – especially among external appointments – it is advisable to add two additional data protection-relevant positions to the DPO: the data protection ambassador and coordinator.

Whereas the Data Protection Ambassador is primarily in charge of technical issues, including compliance with ‘Privacy by Design’ to implement actual IT solutions, the Data Protection Coordinator (DPC) has an overarching role. A DPC is the interface to and the mouthpiece of the DPO for individual departments within an organisation. They assist in making sure that necessary data privacy concerns are still adhered to and carried out even if the DPO is not around. We strongly recommend that all the specified roles work in close cooperation with the Information Security Officer (ISO), in order to ensure data security. Furthermore, if an organisation wishes to achieve constant management attention towards data privacy, one solution would be to have direct/indirect representation at board level by a board member with appropriate knowledge, or by placing the control function of data privacy at the top management level of the company.

## Organisation

Once the personnel roles have been appointed, data privacy can be represented in the form of a “data privacy committee”. In a similar way to an IT or risk committee, this committee should meet at least once every quarter as well as on an ad hoc basis should an incident occur or there are key issues to discuss. We would recommend that a committee comprises (at least) of a director, DPO, ISO and risk manager, as well as a member of staff from the legal and HR department. The committee’s decisions and objectives should be communicated to the company on a regular basis and persons charged with the end-to-end responsibility of seeing through their actual implementation.

Ensuring that data privacy is implemented is one of the organisational measures required, and is not simply achieved by announcing and “filing” data privacy policies as frameworks for all data protection activities. Guidelines and rules have to be ‘baked’ into work processes and tested in regular workshops with employees, in order to demonstrate data privacy processes in the organisation and thus deal with data protection errors on a long-term basis. Staff involved in the workshops can then understand the processes, and suggest possible improvements as well as identify or amend unnecessary processes or steps in any particular process. Any adjustments made need to be written down in the record of processing activities. Ideally, workshops should take place every six months at the beginning and then annually.

---

appointing Data Protection Ambassadors and Coordinators allow end-to-end responsibility for data privacy.

---



---

representation by a data privacy committee is necessary to ensure that organisational measures are implemented effectively and efficiently

---

The second stage involves expanding the policies. The data protection policy is complemented by Data Protection Guidelines, which is then essentially acknowledgement by the board of directors' commitment to data privacy and is directed outwards to customers, partners and supervisory authorities. Then there is the contract register that checks key outsourcing contracts relating to data processing activities, security of processing or third-country regulation. Data privacy requirements for suppliers are taken into account in the supplier guidelines as well as the procurement strategy. Depending on the focus of the business, other aspects of data privacy can be outsourced in additional policies, including cookies, backups or consent management.

data privacy implementation in an organisation is only manifested when policies are actively applied and workshops carried out

**Technology**

As far as the technical side of things is concerned, data protection measures need to be, first and foremost, sustained as efficiently as possible and all processes should be checked for data privacy needs. Can time limits for erasing data be implemented using technology? Will all the principles such as 'Privacy by Design' and 'Privacy by Default' be adhered to? Privacy by Design can be achieved, for instance, by means of an IT infrastructure with switchable encryption 'at rest and in transit', as well as with pseudonymisation. Privacy by Default can be implemented by programming default data privacy-friendly settings such as 'opt-in' or consent management solutions. A Data Ambassador can help in identifying and introducing necessary technical measures.

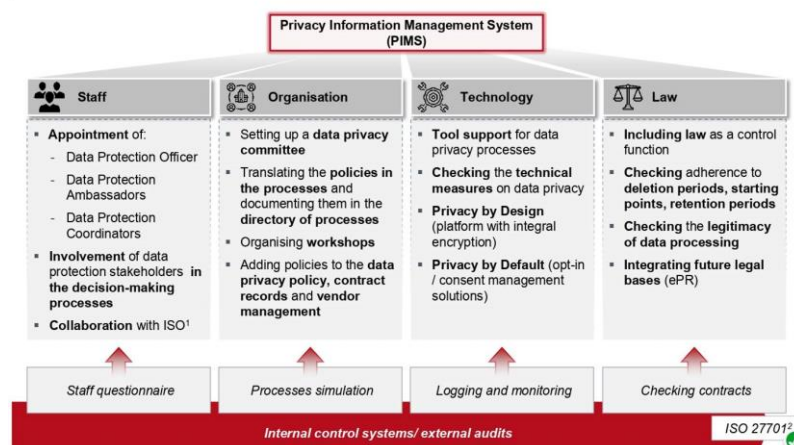
**Law**

Due to the seemingly complex nature of data privacy, we recommend working very closely with the DPO and ISO, as well as the legal department. After all, checkpoints, such as control of important contracts and processes, adherence to time limits for erasing data, starting points, retention periods, as well as the existence of a legal basis for processing personal data, can be guaranteed. Part of this level includes taking into account future regulations such as the ePrivacy Regulation and transferring it to other levels.

a combination with legal expertise leverages TOM for extensive data privacy compliance

To summarise, we would recommend the following aspects are considered when setting up a PIMS:

Key measures for setting up a PIMS and attaining certification



Source: COREsearch (2020) | 1 Information Security Officer | 2 Certification option based on certification according to ISO 27001

Figure 18: To set up a PIMS and attain certification capability, measures from four business dimensions are recommended

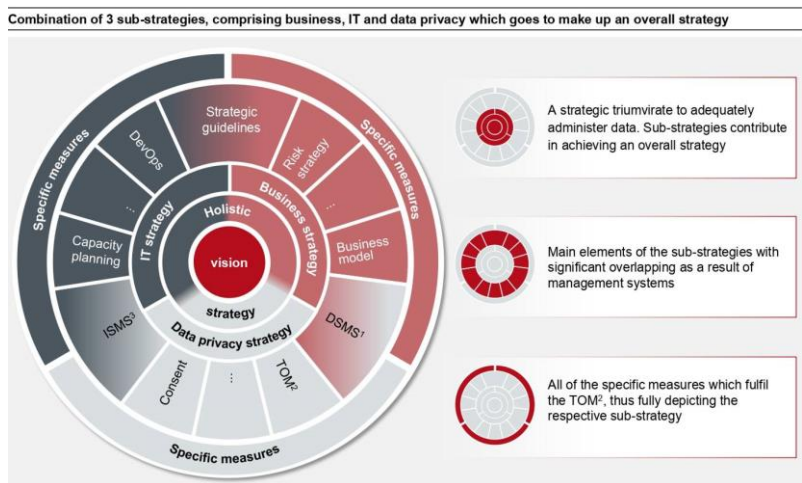
We would also advise measuring the functionality of PIMS across all levels, and deriving potential for improvement. Standards such as ISO 27004 can be enlisted for this. By setting up a PIMS, the company is not only autonomous in the application of data privacy amongst the competition but achieves eligibility for certification in data privacy into the bargain. It is not possible to get official GDPR certification at the moment because resolutions for approval of the European supervisory authorities are still pending. Nevertheless, companies can now be audited for data protection compliance under ISO Standard 27701. A prerequisite is that an Information Security Management System (ISMS) has been set up in line with ISO Standard 27001. The “simple and secure” certifying option thereby achieved lays the foundation for the way in which the company and its employees have, from the outset, to introduce a climate of change regarding data privacy in all aspects concerning the company and interested parties, including customers, staff, business partners and the supervisory authority.

a Privacy Information Management System for more autonomy in handling data – the basis for external certification

### 4.1.3 Data privacy as an integral part of the overall strategy

Although many companies have an IT strategy as part of their overall strategy, both of which are based on regulatory law, for example in the finance sector by the German supervisory authority by way of BAIT, VAIT and KAIT, most of them do not have a dedicated privacy strategy. As far as we are concerned, this is very much recommended in order to gain possible competitive advantage. The third stage of the 3-step model involves adopting an integrated overall strategy by harmonising the business, IT and data privacy strategies. This step anchors data protection in the portfolio of services and thus the business objective. Certification is a sign of sure-fire success and a “must” in terms of a company’s strategic self-image as having control over its data. The company positions itself as a strategic and trusted partner for customers, securing its competitiveness and ability to innovate in the long term while maintaining the efficiency required by means of synergies gained from harmonising its strategies.

data protection and information security as elements of the overall strategy



Source: COREresearch (2020) | 1 Privacy Information Management System | 2 Technical and organisational measures | 3 Information Security Management System

Figure 19: Integral data protection is best achieved by an overall strategy which combines a business, IT and data privacy strategy

Data protection can now be used as leverage for competitive advantage and for maintaining flexibility and innovation in the long term. This aim can be abbreviated to the mantra “you must live (and breathe) data privacy to profit from it”.

Classifying the company’s ambitions in terms of business objectives, IT infrastructure, information security and data protection has to lead to an integrated corporate strategy, from which the aim emerges of positioning data privacy in face of the competition.

*Harmonising data protection with business and IT strategies to form an overall strategy*

Firstly, the dependencies, and their impact on processing personal data, are analysed among the stakeholders – notably users, partners, investors, regulatory authorities, supervisory authorities – and the company. Then an individual target image has to be defined in handling personal data and a comparison made with the goals of existing strategies. By harmonising dedicated points of contact for the strategies regarding primary functions such as product, marketing, procurement, IT, information security and supply management, as well as key supporting functions, including finance, information systems and Human Resources, these strategies are focused on their application. By taking the decision in favour of data privacy compliance, the positioning of the user as a trustworthy partner has already been preselected at the “Basic” stage. The trust pledge must then be substantiated. To achieve strategic positioning of data privacy, the stated strategies are unified around the privacy strategy to form an overall strategy. In this respect, data privacy is on par with all the other strategic goals.

---

harmonising specific sub-strategies on data privacy to create an overall strategy

---

*Strengthening the organisation in accordance with the importance of data privacy within the overall strategy*

The organisation needs to have additional overall strategic goals, in order to embed data privacy within the business. Embedding and placing data privacy on the same level as governance needs to be agreed individually in addition to the legally prescribed roles. However, it is pertinent that the DPO, which has already been introduced at the “basic” level, has a permanent seat in committees which decide on data protection compliance. Further organisational measures involve the following aspects:

---

Data Privacy and Security Ambassadors as partners for developing IT solutions

---

- › Data Privacy Ambassadors to define overriding data privacy requirements
- › Security Ambassadors to advise software developers on implementing Privacy by Design as an integral part of an agile development team
- › Setting up data privacy guilds to enable a professional exchange throughout the company

Both ambassadors are experts in IT security and data privacy. They do not act as controllers of the developers, but rather as partners – this is critical for success.

*Harmonising the processes*

After the strategies of all stakeholders have been harmonised and expanded to include the data protection strategy, and the organisation has been enhanced accordingly, the final step is to harmonise all relevant processes with regard to data privacy concerns. A whole host of processes and challenges concerning IT have to be considered as a result of GDPR requirements. These include, e.g. amended requirements in the execution of data processing or the need to convert the internal system landscape. What makes data privacy more difficult to implement is the fact that the IT infrastructure is often antiquated (see chapter 4.2) because without efficient and secure IT, data protection in a digitalised world is an empty promise.

data security and data protection cannot be separated – they are both closely interwoven

The processes involved in a data-driven activity comprise business and application processes; the latter stem from back-end and front-end processes. Most important is one group of business processes: Information security processes play a direct role in satisfying data privacy requirements, first and foremost TOM. The necessary protection of information (not only personal data) requires information security measures which are organised, in the best scenario, as an Information Security Management System that is based on the ISO 27001 standard. By implementing the information security measures, a large proportion of TOM measures pertaining to data privacy have already been implemented. A data privacy incident occurs if personal data is stolen as a result of a cyberattack (data breach). In this case, both information security as well as data privacy are affected. Consequently, ISMS and PIMS should be harmonised. The better a company's IT/information security, the lower the need to adopt TOM especially for data protection; information security then leverages data protection as data security in the best sense of the words.

TOM combines data protection with data security

Compliance with mandatory regulations with the help of an Information Security Management System (ISMS)			
Goals of Art. 32 GDPR <sup>1</sup>	Selection of security goals and HLS from ISO 27001 <sup>2</sup>		Selection of security goals and HLS from ISO 27001 <sup>2</sup>
Physical access control, logic access control and control of data in transit/at rest	A 09	Access control	Data entry check Transmission check
	A 11	Physical and environmental security	
Separability User check	A 06	Organisation of information security	Availability check, Reliability, resilience, recoverability
	A 09	Access control	
	A 13	Communications security	
	A 14	System acquisition, development and maintenance	
Transport check, storage check, Data medium check, forwarding check	A 09	Access control	Check Order supervision Data integrity
	A 10	Cryptography	
	A 12	Operations security	
	A 13	Communications security	
	A 15	Supplier relationships	
	A 09	Access control	HLS 9 Performance
	A 08	Asset management	
	A 12	Operations security	
	A 12	Operations security	
	A 16	Information security incident management	
	A 17	IS aspects of business continuity management	
	A 06	Organisation of information security	
	A 06	Organisation of information security	
	A 12	Operations security	
	A 15	Supplier relationships	
	A 18	Compliance	

Source: 1 GDPR (2018), Article 32 | 2 ISO/IEC 27001 Standard (2013)

Figure 20: Positive impact on creation of TOM and PIMS by setting up an ISMS



In this stage the company can position itself as a strategic partner of trust for customers and business partners, has secured long-term competitiveness and innovation in the data economy and has laid the foundation for long term cost reduction as a result of the harmonisation and interaction of IT, data security and data privacy. A certification, prepared by establishing the PIMS during the second stage, is now a must, since data privacy is part of the company's strategic portfolio.

#### 4.2 Modern IT architectures automate data privacy and data security

A lot of the mishaps related to data privacy over the past few years were not actually the result of malicious exploitation of customer data but rather due to technical measures that were inadequate for the Internet age such as missing encryption or a lack of password hashing. Databases with sensitive data were very often inadequately, or not at all, safeguarded on the Internet. The fact that safety-related measures are not taken into account can often be traced back to historical system designs, as many systems in the past were not designed to be connected to the Internet. Consequently, a simplified set-up was favoured without extensive security features – this was also due to the absence of pressure from the regulatory and supervisory authorities.

In hindsight, this inadequacy, which can be considered a deficit, is referred to as a technical debt in technology management. In principle, technical debt in IT architectures cannot be prevented without continuous improvement of the system landscape and technology management. Sectors, which have been using IT for a comparatively long time are therefore particularly affected by technical debt: Databases in the public sector, but also system designs dating back to the last century used in banks and insurance companies. These systems were continually extended and equipped with additional functions, for which they were not originally designed; this technological sedimentation leads, in principle, to systems which can only be further developed with disproportionate effort and whose upgrading for use in publicly accessible networks is expensive, time-consuming and complex. A new build from scratch can often be cheaper than further development, as the necessary investment costs increase in proportion to the age of the systems because old IT architectures do not participate in technological progress.

Modern architectural approaches in IT already address many of the data protection requirements. Examples for this include:

- › As cloud technology does not generally involve a separation of spheres of processing and the infrastructure is basically sourced through third parties, all modules have to be protected against electronic access and from being transmitted, and all data needs to be encrypted
- › Kubernetes, as a possible basis for lots of current system designs, manages all aspects of the underlying hardware: hard drives, network, CPUs, memory. Since these resources are normally virtualised and mapped dynamically onto physical hardware, end-to-end encryption is fundamentally essential for multi-tenant systems (which is generally the case with a lot of public Cloud providers)

---

legacy infrastructure is disadvantageous in data economies

---



---

modern technology integrates solutions for data privacy and data security

---

- › Modern systems offer a variety of options for secure data storage, from hardware encryption of physical hard disks, which is almost universally available, to additional encryption of the virtual hard disks (where both provider-managed keys and Bring Your Own Key (BYOK) scenarios can usually be implemented), to a database or field encryption.
- › The same is true of network traffic: from security components
- › such as Cillium for the encryption of network communication at OSI layer 3 and/or 4, up to service meshes such as Istio for encryption at the application layer, there are lots of different options for raising the level of security which previously required a huge effort to implement. Service meshes are able to ensure point-to-point authentication of certain services via mTLS and monitor all connections transparently -without having to adapt the applications. As a result, many aspects of security can be controlled separately from business logic and with fine granularity, with a correspondingly lower probability of error during the implementation phase

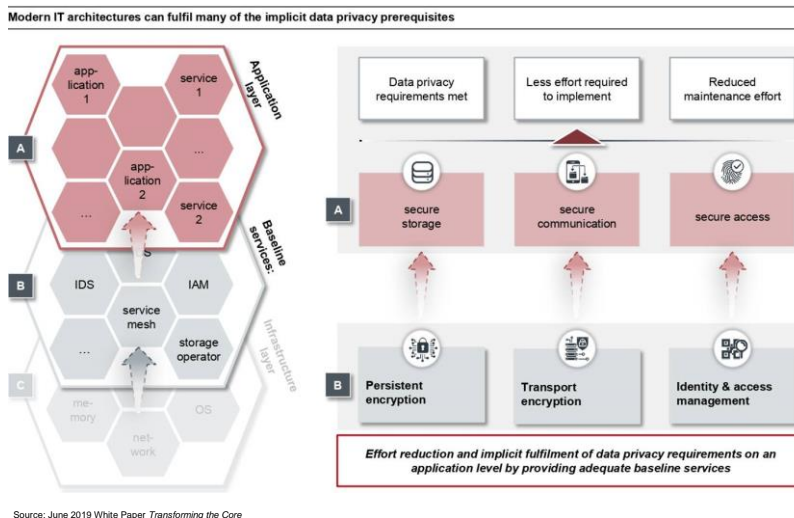


Figure 21: Modern IT architectures help in reducing time spent on and implicit fulfilment of data privacy prerequisites

In short: modern IT architecture designs enable business stakeholders, architects and developers to design secure systems without the need for significant budgets for function development, and as lots of the frameworks have basically become industry standards, improvements made to individual components also benefit their own system without having to devote their own resources to it. Technology management which has been geared towards continual improvement can implicitly fulfil lots of data privacy requirements thanks to modern IT architectures. This means that the focus can be placed on business; data privacy and data security are fulfilled in the background by means of a modern technology stack.



### 4.3 Notes on data privacy practice

There must be an in-depth understanding of key supporting topics for a successful implementation. That is the reason for now explaining the topics of cryptography, pseudonymisation/ anonymisation and information security. These topics cannot be overestimated in terms of their importance to data protection, although we feel that these need a structured classification in order to be able to use them appropriately in practice.

key technical aspects for data protection have long been known and proven

#### 4.3.1 Cryptography for data protection

GDPR is the very first Data Protection Act that talks of “encryption” as a suitable security measure for personal data. Cryptography offers a manageable number of methods on which the complete Internet-based economy is based. Figure 22 shows the cryptographic methods for the privacy goals of confidentiality, integrity, authenticity and non-disputability. Hashing is not a privacy goal in itself; nevertheless, hashes have a key role to play in the cryptographic chain, hence they must be listed and their use in data protection described below.

five cryptographic primitives form the backbone of security on the Internet

Summary of cryptographic methods – only confidentiality and hash are relevant for data privacy

● Guaranteed protection objective    
 ● For the assignment rule, at least two functions are known, de-pseudonymisation is possible

Method	Confidentiality			Integrity	Authenticity	Non-deniable	Hashing
	technical	org.	legal				
Digital signature				●	●	●	
MAC (Message Authentication Code)				●	●		
Symmetric encryption	●		●	●	●		
Asymmetric encryption	●		●				
Hashing	● <sup>1</sup>						●
Pseudonymisation (in line with GDPR)		●	●				
Risk-minimising pseudonymisation		●	●				
Anonymising pseudonymisation	●		●				
Anonymisation	●		●				

Source: COREresearch (2020) | 1 if Urbild is secret

Figure 22: Various protection objectives are addressed depending on which cryptographic primitives are chosen

Encryption (privacy goal – confidentiality of communication and storage) can be symmetric (a secret key for both the sender and recipient) or asymmetric (one pair of keys each – private and public key – for the sender and the recipient). The symmetric variant provides both safeguarding of confidentiality as well as integrity (data cannot be changed and authenticity). Sending and receiving is the same as saving and reading. Consequently, encryption can also be used as a data privacy measure to effectively limit the number of people and services that are entitled to read the content of personal or particular protected data by making the secret key accessible only to authorised persons and services. Unauthorised access can be safely precluded subject to secure storage of keys, e.g. by means of a hardware security module (HSM).

---

If the last two of the aforementioned privacy goals are to be implemented by means of asymmetric encryption, then a digital signature is required. This is the only cryptographic method which also has the non-disputability privacy goal, i.e. the sender of a digitally signed message cannot deny being the author of said message. Whereas the digital signature is based on asymmetric cryptography, a MAC (Message Authentication Code) uses symmetric cryptography and safeguards both integrity and authenticity but not non-disputability because the secret key used must be known to at least two of the communication partners, meaning that the origin of a message cannot be attributed solely to one person.

All classic privacy goals can be implemented with these four methods. Hashing still plays a key role in IT security. Hash functions are one-way functions that store a large volume of data (the “archetype”) as a small volume of data without being able to infer the original from this small amount of data. In practice, data of any size is mapped to 160-512-bit data blocks called hashes. So-called cryptographic hash functions are mainly used today; these are collision-resistant and do not offer any way of calculating the archetype. Nevertheless, the same archetype is always depicted on the same hash, meaning that the hash becomes a fingerprint of the archetype.

---

hashing is overrated in its use in data protection

---

Hashes are not used for affording confidentiality even though this is mathematically possible. The main function of a hash is to check the integrity of the archetype. The second function is the hash signature as proof of authorship (authenticity) of an archetype. Furthermore, the hash function is used to save passwords. The password itself is not saved, only its hash, meaning that a hacker is not able to ascertain the original password even if they have gained access to the hash. The chat platform Knuddels was forced to pay a fine of EUR 20,000<sup>19</sup> in late 2018 because it had stored passwords as plain text which were stolen in a cyberattack. For effective data privacy, a random value (‘salt’) is added to the password before the hashing takes place. This makes life more difficult for the hacker.

The special uses of data protection are differential privacy and pseudonymisation (chapter 4.3.2). Hashing for the purpose of pseudonymisation only makes sense if the variation in input is a large. In technical terms, this corresponds to the same requirements as a good password, i.e. it must not be too short. At least 10, or better still 16 alphanumeric characters – to be on the safe side. In this respect, hashing postcode, birthday dates or even street names for pseudonymisation makes absolutely no sense in data protection, as a hacker can quickly calculate the hashes himself and compare these to the one they are looking for.

---

<sup>19</sup> Regional Data Protection and Information Security Officer for the state of Baden-Württemberg (2018), 03.05.2020

### 4.3.2 Pseudonymisation and anonymisation

Pseudonymisation is still very much an unknown factor in practical data protection. Conversely, this means that there can still be a great future for pseudonymisation in data protection. The GDPR does not distinguish between the various technical, organisational and legal options for maintaining the allocation rule when it comes to “use of additional information” (allocation rule). This can remain with the person, who has undertaken both the pseudonymisation as well as processing the pseudonymised data. It can, however, also be stored in a different department of the same company or externally, either with or without a notary role. Ultimately, the allocation rule can even be securely deleted in legal and technical terms, meaning that anonymisation is achieved. Consequently, one person can be in charge of carrying out the three functions of pseudonymisation or they can be split among two or three controllers:<sup>20</sup>

- Controller 1 (V1) carries out the pseudonymisation
- Controller 2 (V2) keeps the assignment rule
- Controller 3 (V3) processes the pseudonymised data

pseudonymisation has the biggest potential for leveraging data protection – if the legislator and supervisory authority adopt smart amendments

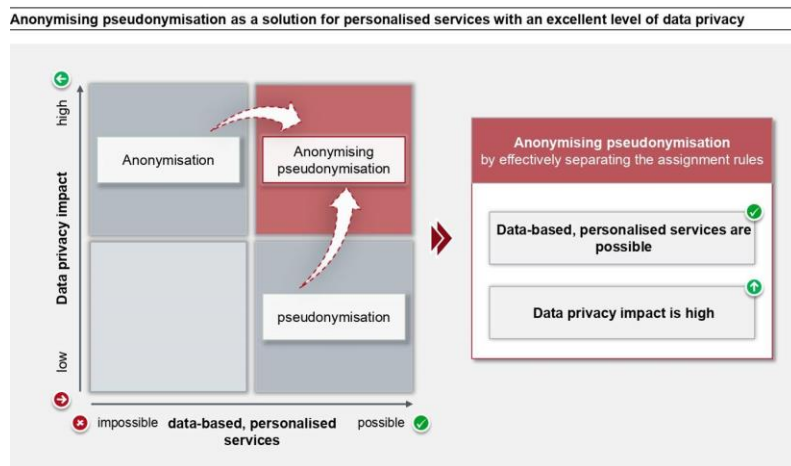


Figure 23: Personalised services with excellent level of data privacy by separating the function of the controllers when carrying out pseudonymisation

If one person is put in charge of all three roles, the safeguarding effect of pseudonymisation is very low, since the data has not been processed personally, but can be assigned at any time. This is also the case if all three roles are split up within an organisation, such as in different departments. If, however, it is ensured, both legally (e.g. in a GDPR amendment) and contractually, that V2 is a notary and the allocation rule in its sphere of influence is safe from access by V1 and V3, then anonymising pseudonymisation is achieved for the two possible combinations of a separated V2. This offers a degree of protection comparable to that of anonymisation but, nevertheless, preserves the option of pseudonymisation or even de-pseudonymisation of data.

<sup>20</sup> Roßnagel (2018).

---

If the allocation rule is discarded, then the data is anonymised. Dividing the roles between three responsible parties V1, V2 and V3 differentiates the possible applications of personal data into three quality levels of pseudonymisation. It remains to be seen which fields of business activity will result from this scope of possibilities.

A major challenge in pseudonymisation is that data records cannot only be assigned to a person via a unique identifier or a person's directly related attributes, but also that a unique combination of attributes, which cannot be used individually for identification, can be used to provide an unambiguous personal reference. In this way, 98% of all US Americans can be clearly identified using a combination of zip code, date of birth and gender.<sup>21</sup> A combination of attributes such as this is termed as quasi-identifier. Quasi-identifiers can be prevented by means of various generalisation procedures. The most important generalisation procedures include k-anonymity, l-diversity and t-closeness, which must always be applied for effective safeguarding of pseudonymised data. In addition to generalisation, data can be randomised by permutation or the addition of noise.

An interesting field of research concerning randomised anonymisation techniques is that of differential privacy (DP). Aggregates of lots of personal data records are formed with the help of DP algorithms, which achieve different levels of anonymisation depending on the configuration of the algorithm parameters. Differential privacy does not allow conclusions to be drawn about a specific individual; personal data is randomised. However, the searcher can get information that they were looking for on a lot of people. This aggregated data can be used, for example, for statistical purposes such as those in line with Recital 162 GDPR.

Nevertheless, the results of processing in the form of a statistical analysis may not be used to make decisions about or take measures against individuals. By contrast to the anonymisation of specific data records, which may be deanonymised by means of certain correlations of information contained in it and/or by adding information from external sources, DP aggregates cannot be deanonymised. This attribute of differential privacy is achieved by three consecutive mathematical methods:

- › Hashing: to conceal original data
- › Subsampling: to limit data to a subset of the original
- › Noise injection: Enrichment with random values (adding noise)

Differential privacy paves the way for new commercial and, at the same time, data privacy-compliant services such as, for instance, data analyses for improved marketing – as successfully implemented by Apple and Google.

---

anonymising pseudonymisation as a new practical solution module

---

---

with pseudonymisation, differential privacy offers a further opening clause for the data-driven economy

---

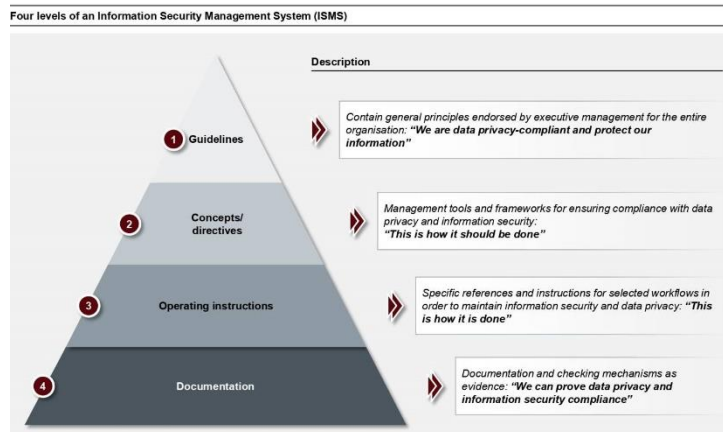
---

<sup>21</sup> Sweeney, Latanya (2000).

### 4.3.3 Information security

Data protection and information security are the two inseparable sides of the same coin. Both sides are linked in the technical and organisational structure via Article 32 “Security of processing”, Article 25 GDPR “Data protection by design and by default” as well as Section 64 Federal Data Protection Act (BDSG)

“Requirements for the security of data processing”. An ISMS consists of policies and processes which the example below (Figure 24) has subdivided into four levels:



Source: COREresearch (2020)

Figure 24: Using the four levels of the Information Security Management System to address data privacy and information security

Information security implemented in an ISMS guarantees data security and serves as a model for the PIMS in terms of organisational, technical, legal and personnel aspects. In the German blog “ISMS nach ISO 27001 – Blaupause für den Einsatz in Unternehmen“ (ISMS according to ISO 27001 – blueprint for use in business), a detailed mode of operation of an ISMS is presented as a tool for data privacy compliance as well as providing information on how to set up a certifiable ISMS in line with ISO 27001.



<https://core.se/de/techmonitor/isms-nach-iso-27001>

## 5 Conclusion

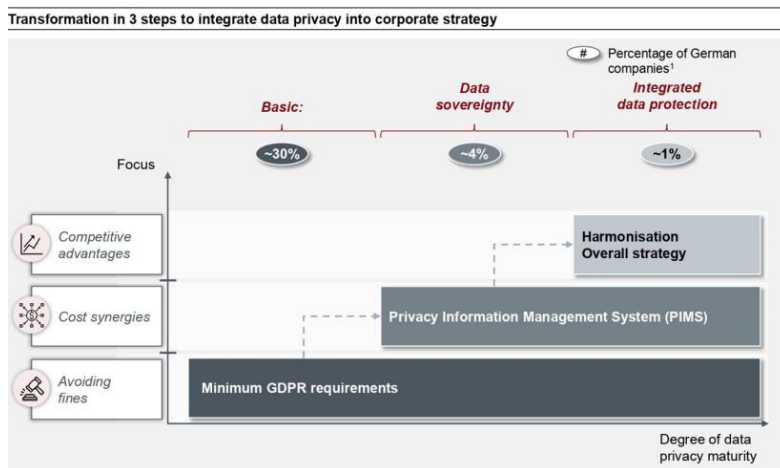
Then unison of data privacy and trust serves as the raw material for a successful digital economy. Technological development can be seen as offering both opportunities and risks. With modern data privacy laws, such as GDPR, the legislator addresses the risks that arise for the end-user. At the same time, the authors of this paper see clear potential opportunities in actively complying with the statutory regulations based on technology. This is also reflected in the opinion of the Federal Commissioner for Data Protection and Freedom of Information (BfDI), Professor Ulrich Kelber. In his opinion, "Data privacy is a protection of fundamental rights that needs to be upheld", and adds "Profiling and tracking are nothing new, modern digitisation is also possible without spying, informational trust is becoming the core issue."<sup>22</sup>

trust is key for a successful business; data privacy establishes confidence

GDPR is being imitated worldwide, and European legislation has been adapted even in technology-friendly California in the shape of the California Consumer Privacy Act. This certainly has not been adopted against the interests of the global technology companies based there.

There is no longer a realistic option to ignore data privacy in corporate governance, as the pressure to impose sanctions is on the increase for all areas of business, current business models may be at risk, or new, innovative data-based services cannot be positioned in the market without adequate data protection. Some market participants like the major platform providers have already taken this to heart and have adapted their business strategies accordingly. The authors feel that European companies should see the benefits of the underlying conditions in competition with Western or Asian competitors as an opportunity. Europe can still lead the way in a data-driven economy based on willingness, transparency and security. This economy cannot be stopped, so we should play a decisive role in shaping it.

Europe as an asset in setting up data-based business models with inherent data privacy



Source: COREresearch (2020) | 1 Experts' estimates COREresearch (2020)

Figure 25: The 3-step data privacy model serves as an aid for sustainable integration of data protection into corporate strategy

<sup>22</sup> Prof. Ulrich Kelber (2020), 26-27.02.2020

---

If data privacy is to be seen by companies as a basis for building customer confidence and is to become an integral part of the corporate strategy, then this can be achieved effectively and efficiently using a 3-step model.

- Basic level 1 ensures compliance with the minimum legal requirements based on a few key levers derived from practice
- The 2nd level looks at the confident handling of data privacy in order to build trust networks with the help of a comprehensive Privacy Information Management System (PIMS). This can also receive external certification and an independent seal of approval in the future
- The third level of a far-reaching data privacy design positions this as an equal component of corporate strategy along with the business and IT strategy

High-quality and efficient solutions at all levels of data privacy and data security can be created using modern IT architectures.

Last but not least, we would like to call on authors to join forces. Cooperation for the customer's benefit and thus economic success must emerge from the conflict between data protectors and data exploiters and the mutual observation of the legislator and the economy. Data privacy is not a necessary evil, but it actively paves the way for opportunities to build customer confidence in products and services in the digital economy. Customers' trust, as the basis for a sustainably successful business, is the valuable raw material that must be secured.

---

a change in perspective: leveraging data privacy

---

## Sources

- Alexander Roßnagel (2018): *Pseudonymisierung personenbezogener Daten – Ein zentrales Instrument im Datenschutz nach der DSGVO*, ZD 2018, 243.
- Accessnow (2019): *One year under the EU GDPR*
- Bitkom (2019): *DSGVO, ePrivacy, Brexit-Datenschutz und die Wirtschaft*
- Bitkom (2019): *Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr*
- Bitkom (2019): *Nutzervertrauen in Datensicherheit im Internet steigt*
- Bundesministerium der Justiz und für Verbraucherschutz (2007): *Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 11 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066) geändert worden ist*
- Bundesverband Deutscher Zeitungsverleger e.V. (2019): *Infotag Datenschutz 05.12.2019*
- BVDW (2019): *BVDW-Mitgliederumfrage zur EU-Datenschutzgrundverordnung (DSGVO)*
- Cisco (2019): *Data Privacy Benchmark Study*
- CMS (2020): *GDPR Enforcement Tracker*, abgerufen am 24.04.2020
- COREresearch (2015): *White Paper: Wollen » Können*
- COREresearch (2019): *White Paper: Transforming the Core*
- Der Europäische Datenschutzbeauftragte (2020): *Entwicklungsgeschichte der Datenschutz-Grundverordnung*
- Die Welt (2018): *So teuer sind Hackerangriffe für Unternehmen*, accessed on 18.05.2020
- Digital Analytics (2019): *Trendstudie 2019*
- Europäische Kommission (2017): *Vorschlag für eine Verordnung des europäischen Parlaments und des Rates*
- European Commission (2016): *Article 29 Data Protection Working Party*
- European Data Protection Board (2019): *Report on the implementation of GDPR*
- FAZ (2019): *Die wichtigste Ressource für Tech-Unternehmen*, accessed on 01.05.2020
- Geldinstitute (2020): *Millionenschäden: Die Kosten eines Datenlecks*
- Handelsblatt (2019): *Grafiken des Monats – 8. August 2019*
- Heise online (2019): *Bundestag: Deutlich mehr Stellen für die Bundesdatenschutzbehörde*, accessed on 15.05.2020
- IDC (2018): *The Digitization of the World*
- IDC (2019): *Industrieunternehmen auf dem Weg in das datenbasierte Tagesgeschäft*
- IDW (2019): *Datenmenge explodiert*
- IDW (2020): *Datenschutz: Ungeliebtes Regelwerk*
- Ipsos (2019): *Internet Security & Trust*
- Irish Data Protection Commission (2020): *Annual Report 2019*
- ISO/IEC 27001 Standard (2013)
- Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg (2018): *LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DSGVO*, accessed on 03.05.2020
- Prof. Ulrich Kelber (2020): *Anlässlich der Fachveranstaltung „13. Praxistage Datenschutz“*, 26.–27.02.2020, Cologne
- Reguvis (Bundesanzeiger Verlag) (2019): *Digital Dialog Insights 2019*
- Sweeney, Latanya (2000): *Simple Demographics Often Identify People Uniquely (Datenschutz Working paper 3)*
- Thomson Reuters (2019): *Survey, GDPR+1 YEAR*
- TrustArc (2018): *GDPR Compliance Status*
- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) in der aktuellen Version des ABl. L 119, 04.05.2016
- YouTube (2019): *Werbevideo von Apple: Privacy on iPhone—Simple as that—Apple*, accessed on 03.05.2020



---

## Authors

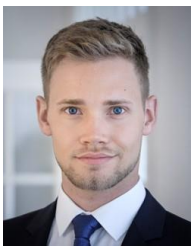


**Magdalena Buski** is a transformation fellow at CORE. She graduated from the Leipzig University of Applied Sciences (HTWK) with a Bachelor of Arts degree in Business Administration. At CORE, her main activities involve the strategic design and implementation of IT transformations and the development of information security management systems in line with ISO 27001.

---

**Magdalena Buski**  
[magdalena.buski@core.se](mailto:magdalena.buski@core.se)

---



**Marc-André Dymala** is a transformation manager at CORE. He has two master degrees, one in International Business Management (SWUFE Chengdu, China) and one in Chinese European Economics and Business Studies (HWR Berlin). His core responsibilities are digital transformation as well as ISMS (ISO 27001) and data privacy.

---

**Marc-André Dymala**  
[marc-andre.dymala@core.se](mailto:marc-andre.dymala@core.se)

---



**Waldemar Grudzien** is an expert director at CORE. His doctorate is in electrical engineering and he graduated with an economics degree (*Diplom*). His main area of responsibility is information security and data privacy – in theory and practice, including operational activities as an ISO and DPO for various customers.

---

**Dr Waldemar Grudzien**  
[waldemar.grudzien@core.se](mailto:waldemar.grudzien@core.se)

---

---

## Author team



**Christian Böhning** is a managing director at CORE. He has many years of experience in carrying out digital transformation projects in industries that are permanently changed by IT. His work focusses on developing programmes for modernising IT architectures, implementing compliance initiatives and realigning IT organisations.

---

**Christian Böhning**  
[christian.boehning@core.se](mailto:christian.boehning@core.se)

---



**Johannes von Bonin** is a transformation associate at CORE. He gained his master's degree in Economics of the Middle East from the University of Marburg and the Lebanese American University in Beirut. His main activities at CORE include digital transformation, agile project and product management as well as data privacy.

---

**Johannes von Bonin**  
[johannes.bonin@core.se](mailto:johannes.bonin@core.se)

---



**Nadine Hofmann** is a transformation associate at CORE. She studied aerospace engineering in Braunschweig (Lower Saxony) and Dresden. Her core area of expertise is the technical side of data protection and information security (focus areas are IAM and Security Operations Center). She assists clients in setting up management systems.

---

**Nadine Hofmann**  
[nadine.hofmann@core.se](mailto:nadine.hofmann@core.se)

---

---

## About

As an independent technology think tank, we investigate the systematics of technologically driven transformations in industries with a high degree of IT in the value creation process. As part of our research activity, we analyse markets and technologies, address the structures, causes and mechanisms of technological change, and curate results for clients and the public

Furthermore, we also present a selection of the results from our interdisciplinary research in the context of comprehensive publications, individual studies and lectures available to the public at large.

## Disclaimer

The contents and structure of our publications are protected by copyright. The reproduction of content, in particular the use of texts, parts of texts or images, requires prior consent. The logos depicted are the property of the enterprises concerned. CORE SE does not hold any rights to the logos, which it has used purely for academic purposes.



---

[https://core.se/de/publications/  
white-paper](https://core.se/de/publications/white-paper)

---

CORE SE  
Am Sandwerder 21–23  
14109 Berlin  
<https://core.se/>  
Phone: +49 30 263  
440 20  
[office@core.se](mailto:office@core.se)

COREtransform GmbH  
Am Sandwerder 21–23  
14109 Berlin  
<https://core.se/>  
Phone: +49 30 263 440 20  
[office@core.se](mailto:office@core.se)

COREtransform GmbH  
Limmatquai 1  
8001 Zürich  
<https://core.se/>  
Phone: +41 44 261  
0143  
[office@core.se](mailto:office@core.se)

COREtransform Ltd.  
Canary Wharf, One Canada Square  
London E14 5DY  
<https://core.se/>  
Phone: +44 20 328 563 61  
[office@core.se](mailto:office@core.se)

COREtransform Consulting MEA Ltd.  
DIFC – 105, Currency House, Tower 1  
P.O. Box 506656  
Dubai | VAE  
<https://core.se/>  
Phone: +97 14 323 0633  
[office@core.se](mailto:office@core.se)

