Data Protection & Industrie 4.0

How to treat personal data on a corporate level

in cooperation with

GvW Graf von Westphalen

VDMA

Editorial

Christian Steinberger

Dear Reader,

Data protection has been on the agenda of companies for some time, and the protection of personal data has become increasingly important for the companies of the machinery and plant engineering sector. With a view to the increasing sensitivity of customers and users regarding their data, high data protection levels are key for every company.

Especially under Industrie 4.0 conditions, data protection will gain in significance: integrated systems, data-dependent automation processes, cloud services and big data are keywords that data protection officers will have to take into account in the near future.

In this context, data protection also means pending changes have to be considered and the expenditure related to integrating these factors into the data protection policies of the company must not be shied away from. This is also necessary as data protection authorities have adopted a more proactive approach and monitor companies for adherence to data-protection rules.

The VDMA has recognised that especially smaller and medium-sized companies find it difficult at times to find their way through the wealth of statutory conditions imposed by the complex and partly abstract requirements of data protection. The present guide is therefore meant to outline the fundamentals of data protection and provide the companies with a useful tool to cope with the protection of personal data in their own companies.

An intrinsic factor of Industrie 4.0 is that data-protection aspects have to be implemented in each project right from the start. We hope that we have succeeded in offering you concise and practical advice that you can readily apply to many situations that you are aware of or that you become aware of.

Christian Steinberger
VDMA Legal Services

Contents

Introduction

Current developments, opportunities and challenges inherent to what is called “Industrie 4.0”, the next phase in the digitization of the manufacturing sector, are often linked to the processing of personal data: The quality and efficiency of a smart factory can be optimised through precise assessment of staff productivity, RFID chips, and machine-fitted sensors offer hitherto unknown possibilities to control and assure quality throughout the entire life-cycle of a product.[1] Yet, they also enable profound insight into the behaviour of staff and end-users of the products.

Data protection law addresses risks such as potential surveillance of staff in the course of production processes or the possible prying of end-users of a product. A careless approach to data protection law bears huge financial risks: Already from today’s perspective, the German Federal Data Protection Act (“BDSG”, the “Act”) imposes fines of up to € 300.000 for each individual breach. The European general data protection regulation will enter into force in spring 2018 and provides that large companies are exposed to fines of up to € 200 million or 4 % of their overall global turnover of the preceding financial year, whichever is higher. Furthermore, companies will face claims for damages by data subjects, injunction suits, penal prosecution and for many companies the highest risk: loss of goodwill.

How fast personal data may be disclosed within an industrial undertaking has been shown by several large-scale companies that where the object of so-called social engineering attacks: In the case of a steelwork, the attackers did not only conquer the office network, but also the production networks.[2]

Compliance in data protection matters is no easy task, especially where personal data are processed in huge amounts and all around the world, as it is customarily the case in Industrie 4.0 technology. The latest endeavours on the European level to come to a data protection convention with the US and the critical and restrictive approach adopted by the European Court regarding data transfer into the US show this only too clearly.

The following guide is meant to facilitate for you, as a member of the VDMA, the access to data protection in Industrie 4.0 and indicate at the same time approaches and further sources of information to minimise your risk and create awareness for data protection issues.

The legal framework of data that do not relate to persons, which are often referred to as “machine data”, is outside the present guide’s scope; the VDMA will prepare relevant publications as the need arises in the course of the impending discussions.

[1] Report summarising the results of the Industrie 4.0 platform, implementation strategy Industrie 4.0, page 45, in German, https://www.bmwi.de/BMWi/Redaktion/PDF/I/industrie-40-verbaendeplattform-bericht,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (last accessed on 12 April 2016)

[2] Federal Office for IT Security, Status Report 2014, p. 31 et seq. and 34 et seq., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile&v=1 (last accessed on 12 April 2016).

1. Bases of data protection in Industrie 4.0

1.1 Data protection

The German and European data protection law is based on the principle that things are "prohibited unless specifically authorised". As surprising as this may sound in the era of Industrie 4.0, this means that, subject to only a few exceptions, processing of personal data is, as a rule, prohibited. The processing of personal data is usually only permitted if there is sufficient justification. Such justification may ensue from the German Federal Data Protection Act or from the consent given by the data subject. The concepts of "processing" and "personal reference" are rather extensive, which means that a large range of Industrie 4.0 applications are affected: Data are e. g. deemed to be processed if personal data are transferred or stored. For personal reference, it is already enough when the date would enable the determination of an individual (for more details, see No. 3.1.2 below).

According to the German Data Protection law, it is, in principle, forbidden to process personal data. A valid justification to do otherwise must be established.

From a formal perspective, data protection law is administrative law, i.e. public law, and government agencies (the "data protection supervisory authorities") will monitor their adherence. Data protection supervisory authorities exist in each federal state and are entrusted with so-called governmental intervention rights. For a company, this means that authorities are not only entitled to make investigations regarding possible breaches of data protection (e. g. upon request of the data subject), but that they may also impose on the company mandatory conditions regarding the processing of personal data and, if an actual breach is detected, even fines.

For a company to be able to fulfil the requirements of data protection law, it must take into account both internal corporate aspects (e. g. protection of personal data of staff, personal data management, appointment of a data protection officer) and external aspects (e. g. enter into agreements on contract processing of data with business partners / supplies / contractors or fulfil certain requirements regarding the processing of personal data in the internet, e. g. data protection declaration on their website).

The yardstick applied by data protection law currently ensues from the German Federal Data Protection Act. In addition, there are specific sector rules and with respect to Industrie 4.0, these are in particular the Telemedia Act ("Telemediengesetz") and the Telecommunications Act ("Telekommunikationsgesetz"). Moreover, a new legal framework will be set on a European level as of 2018 when all the Member States of the EU will be subject to the general data protection regulation.

1.2 Industrie 4.0

Industrial production in the context of Industrie 4.0 is characterised by extensive IT integration, the comprehensive use of sensors, actuators and novel analytic methodologies. The aim is an approach to production based on integration and local organisation that is also self-optimising.[3] The smart factory is driven by the combined use of innovative technologies such as the internet of things, cyber physical systems, cloud computing and big data.[4]

These innovative technologies entail quite a number of challenges from a data-protection point of view, as Industrie 4.0 production usually generates an added value out of combining various individual data, and more often than not references may, or are even intended to be inferred regarding individuals (e. g. staff, end-users or even other third parties affected by sensors), which may enable the creation of profiles of data subjects. The aspects shown in the following chapters should therefore be considered as early as possible in an Industrie 4.0 environment and adapted to the individual circumstances.

The production methodology of Industrie 4.0 ideally requires that data protection aspects are already included in the planning phase.

1.3 Areas concerned

Data protection law is also an interdisciplinary set of rules. It concerns various other areas of law, such as labour law and penal law, and technological aspects such as IT security. The last aspect in particular is of much importance for Industrie 4.0 manufacture. Data protection law in this respect demands that the technological and organisational measures are adopted that are required in the light of data protection law and in this respect imposes various conditions. The required level of IT security must be ensured in each step of processing of personal data (and not only e. g. in the context of contract data processing). For details about the question of IT security requirements, one can, among other things, refer to the technical and organisational data security measures mentioned in the Data Protection Act attached as Annex 9. We also make reference to the VDMA guides on information security (parts one and two) that members can obtain free of charge from the association's publishing house.[5]

In Industrie 4.0, IT security also serves the purpose of protecting personal data.

[3] Fraunhofer ISI, Industrie 4.0 – 10 propositions from the perspective of innovation research, December 2015, in German, http://www.isi.fraunhofer.de/isi-wAssets/docs/profil/de/Industrie_4_0-Thesen.pdf (last accessed on 11 April 2016).

[4] Regarding individual terminology, cf. Research and Innovation Expert Panel, expert opinion 2016, page 145 et seq., http://www.e-fi.de/ (last accessed on 16 Apr 2016).

[5] Part 1 can be downloaded from http://www.vdmashop.de/Informatik-und-Technik/Leitfaden-zur-Informationssicherheit---Teil-1--Sensibilisierung.html
Part 2 from http://www.vdmashop.de/Informatik-und-Technik/Leitfaden-zur-Informationssicherheit-Teil-2---download.html

2. What data protection provisions are applicable to the / your company?

Prior to processing personal data, the company must find out whether, and if so, what data protection law is applicable. This is particularly challenging with respect to the processing of personal data on an international level, which is nothing unusual in Industrie 4.0.

German data protection law uses the concept of the "controller". A controller is any person or body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same. It is worth noting that data protection law does not provide for a group privilege, i.e. that even in the case of personal data being transmitted from the subsidiary to the parent company, it is necessary to create an independent legal basis under data protection law.

Also where personal data are communicated within a group of companies, this does require a justification and needs to be called into question. On an international level, even more stringent requirements apply.

In the framework of international data processing, an assessment must be made whether the applicability of German data protection law would be superseded by the application of the data protection law of another European state. This may be the case if the controller is located in another Member State of the European Union or another contract state of the European Economic Area (EEA) and although data are collected in Germany, this is not performed by a German subsidiary. Yet, if a non-European company would collect data in Germany, the German Federal Data Protection Act will be directly applicable. Then, an assessment must be made as to whether the non-European country does or does not accord an appropriate data protection level from a European perspective. Only in the affirmative will it be legally possible to transfer data (if relevant justification is available). In all other cases, it has to be assessed whether the level of protection can be ensured through technical and/or contractual mechanisms. This assessment is always an individual assessment and must be made by specialists.

The ongoing discussion on a European level regarding the safe harbour convention between the EU and the US that has been declared unlawful by the European Court and the discussions in the adopting process of its successor document, the privacy shield, show that there will be no uniform solution.

3. What are the duties of the / your company?

If it has been established that the data protection law, and, if appropriate also the potential of data processing in the international context, is applicable, the company must comply with the duties outlined hereinafter.

3.1 General data protection law

Section 4 of the Act provides that the processing of personal data is admissible only if permitted by the Act or any other legal provision or if the data subject has consented. For example, the Act allows that data are collected and stored for own commercial purposes pursuant to Sec. 28 of the Act. Yet, the provision stipulates a large range of additional requirements that must be fulfilled to make data processing lawful. Hence, in the individual case, data processing may only be considered lawful if needed to create, carry out or terminate a legal obligation or quasi-legal obligation with the data subject. The purposes for which the data are to be processed or used have to be expressed in concrete terms, at that. Using the data for other purposes is only possible if certain, narrowly defined requirements are fulfilled (e. g. in so far as this is necessary to safeguard justified interests of the controller of the filing system and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use).

The processing of personal data may be permitted on the basis of a statutory exemption or consent by the data subject.

The general data protection obligations do not only refer to the above-mentioned safeguarding of IT security (cf. No 1.3 above), but also to the appointment of a so-called corporate data protection officer.

A corporate data protection officer needs to be appointed if

- usually more than nine persons are deployed to carry out automated processing, use or collection of personal data; or
- usually more than twenty persons are deployed to carry out processing, use or collection of personal data in another way, e. g. through manual processing.

If and when required, a group must appoint data protection officers for every group company separately; it may be advisable to appoint also a group data protection officer. The data protection officer must report directly to the corporate management and must be equipped appropriately. The person appointed must possess the specialised knowledge and reliability necessary for such office. The data protection officer shall not be subject to instructions, suffer no disadvantage though the performance of his / her duties and enjoys protection from termination pursuant to the provisions of Sec. 4(f) No. 3 of the Act. Due to the substantial expenditure related to the office of the corporate data protection officer, it may be appropriate not to appoint a member of staff, but an external corporate data protection officer (e. g. a specialist lawyer).

Each company must make an assessment whether it is under the obligation to appoint a corporate data protection officer. Due to the related privileges, it may be advisable to appoint a third party as corporate data protection officer.

Further general data protection duties refer to intended reporting methods of automated processing, e. g. with respect to HR measures, however only if and when no corporate data protection officer is appointed.

To avoid complex and tedious reporting obligations for each existing procedure of automated processing, it is highly advisable to appoint a corporate data protection officer.

Furthermore, it is necessary to carry out prior checks as provided for in Sec. 4(d) No. 5 of the Act if automated processing operations present special risks to the rights and freedom of data subjects (e. g. when health data are processed or processing is performed for the purpose of performance assessment). And there are also specific duties to notify data subjects, e. g. when data are stored for the first time for own business purposes without knowledge of the data subject, Sec. 33 of the Act, or in the event of unlawful access to data, Sec. 42(a) of the Act.

3.1.1 Persons

3.1.1.1 Members of staff

Sec. 5 of the Act provides that all employees of the company interested with the processing of personal data are required to give an undertaking to maintain data confidentiality on taking up their duties. Data confidentiality is to be understood as the prohibition of an unauthorised collection, processing or use of personal data. As a rule, this duty should be imposed already upon recruitment together with the employment contract on all members of staff, because a person can be deemed “entrusted with data processing” when simply using a PC that would also enable access to personal data (e. g. in the case of using an email programme). In the Industrie 4.0 context it is particularly advisable to consider also obliging employees with respect to the secrecy of telecommunications pursuant to Sec. 88 Telecommunications Act. The secrecy refers to the contents of telecommunications and its specific circumstances, in particular the fact whether a person is or was involved in a telecommunications process. The secrecy of telecommunications also extends to the specific circumstances of unsuccessful connection attempts and may therefore be applicable to many Industrie 4.0 applications.

In this context, it must also be verified whether consent declarations by staff regarding the processing of personal data and / or works agreements are required and in effect in the individual case. The processing of personal data, in particular in the Industrie 4.0 context, is a legal process that requires an authorisation; yet, the Act only provides for insufficient legal bases in many cases (Sec. 28 and 32). Consent is subject to stringent requirements in order to be effective (see No. 3.2 below for details).

Furthermore, staff should be trained on a regular basis regarding their duties when dealing with personal data.

3.1.1.2 Customers

The processing of customer data becomes relevant for Industrie 4.0 e. g. with respect to product life-cycle management, when the end-product communicates with the manufacturer and thereby communicates data from which facts about individuals (e. g. owners of the product) can be inferred. Furthermore, data protection questions arise about customer data management, e. g. when sending out promotional emails or using the company website or if customer databases are to be resold. It always has to be verified whether there is a justification for the processing of personal data (through statutory basis or consent). When promotional mails are sent out, not only the statutory data protection requirements have to be taken into account, but also the stringent requirements of the German Act on Unfair Competition ("UWG").

The use of personal data in the context of product life-cycle management and each promotion activity have to be assessed in the light of data protection; usually, the data subjects' consent will be required if personal data are processed.

3.1.1.3 Business partners / suppliers

To the extent that business partners and suppliers are concerned, steps must be taken to ensure that they will not incidentally be able to process or access personal data from the company without legal basis. To do so, it may become necessary to enter into agreements on contract processing of data pursuant to Sec. 11 of the Act with the contractor, e. g. for IT maintenance or planning and ordering IT projects. If drafted and used in the correct way, these agreements safeguard that the company continues to be the controller and that communications in this respect are no unauthorised transfer of personal data to a third party, but a permitted case of contract data processing.

A similar constellation arises in an Industrie 4.0 environment where specific components are personalised by another manufacturer in such a way that personal data are embedded. In such a case, it may also be advisable for the principal intermediary to opt for contract data processing (then as the contractor).

3.1.2 Data

What data in an Industrie 4.0 application will be classified as personal data is laid down in Sec. 3 (1) of the Act. Data protection law is only applicable if the data used has a personal reference. The law has the following definition for personal data:

Personal data means any information concerning the personal or factual circumstances of an identified or identifiable individual (the data subject).

The term is understood in a broad sense and by no means restricted to “classical” personal data such as name, address and date of birth. Other identifying data must not be neglected, e. g. movement data, personal features, IP address (contentious) and biometric data, always independent of format and carrier medium. For a personal reference to exist it is sufficient that an individual can be determined, therefore Industrie 4.0 manufacture must exercise particular care and diligence in making the required individual assessments: A large range of what might at first sight be irrelevant data may be earmarked by the authorities as having a personal reference if the information could basically (also taking into account additional knowledge that the supervisory authority does not have to assume to be actually available in the company) be allocated to a person.

A large range of what might at first sight be irrelevant data may be earmarked by the authorities as having a personal reference; a detailed, individual assessment is required in each case.

Additional conditions apply when special categories of personal data are processed; these are information on a person”s racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life. In so far as such personal data are processed, the consent must refer expressly to these data. If data are intended to be processed without consent but on a statutory basis, the risks to which the data subject is exposed must be assessed in a prior check pursuant to Sec. 4 (d) No. 4 of the Act.

3.1.3 Measures

The following, often simple measures facilitate the lawful processing of personal data: First and foremost this concerns the appointment of a corporate data protection officer (internal / external). Pursuant to the principle postulated by Sec. 4 (g) of the Act, the data protection officer has to work to ensure compliance with the Act and other data protection provisions, e. g. through monitoring the lawful application of data processing software.

Each company must make an assessment whether it should appoint a corporate data protection officer. In many cases, this is advisable, although there is no statutory obligation.

Another aspect when implementing data protection requirements concerns the preparation of procedure registers. These include – for internal use and towards governmental authorities – the best possible compilation of all procedures with data protection relevance, and they must fulfil, among other things, existing documentation duties pursuant to Sec. 4(d) and 4(e) of the Act (the comprehensive internal procedure register is also sometimes referred to as processing overview). A part of the comprehensive procedure register then has to be made accessible to anybody upon request by the data protection officer. Further measures to promote data protection compliance are the company policies, potentially also works agreements and training offered to and attended by staff.

3.2 Special features in the Industrie 4.0 company

The use of Industrie 4.0 technologies (e. g. internet of things, big data) has it that in production data are increasingly generated, transmitted and processed digitally, potentially even by the products and / or the production equipment themselves or through external platforms. Hence, many more additional data are created that, due to their identification potential (specifically regarding staff and end-users) may be subject to data protection provisions (cf. in this respect No. 3.1.2 above).

Moreover, often external persons (e. g. IT service providers, computing centres, cloud services providers) are included in digital production processes. To the extent that external persons come into contact with personal data, a mandatory check must be conducted as to whether this is admissible on a statutory legal basis or on a consent basis and whether an agreement on contract data processing has to be considered (cf. in this respect No. 3.1.1.3 above).

Further challenges exist from a data-protection point of view if data are to be processed outside the European Union or the European Economic Area. If this is the case, an assessment of the applicability of data protection law and the protection level provided in the non-European jurisdiction must be made, and for such processing more stringent requirements apply. In some cases, it may become necessary to enter into additional agreements with the external party – e. g. the standard clauses of the European Commission for the transmission of personal data into third countries.[6] In this respect, the admissibility has to be assessed in each individual case, because European jurisdiction has stringent requirements the third country's protection level has to fulfil, and more often than not the data transfer will be found inadmissible. Wherever possible, it should be considered to restrict data processing to areas with European jurisdiction.

If possible, the processing of personal data should take place where European law is applicable.

If the data subject's consent is to be used as the required legal data protection basis (as to the requirements, see No. 1.1 above), Industrie 4.0 must also take into account that only an "informed" consent will be legally valid. The data subjects must therefore be fully aware of the consequences of their decision and in this respect of the purpose and scopes of application of the data utilisation. These requirements are often quite difficult to fulfil, e. g. in the case of big data.[7] So if in the individual case a declaration of consent is considered, an expert should be consulted (e. g. corporate data protection division, data protection officer, specialist data protection lawyers).

Specific requirements must be fulfilled for consent declarations to be valid. In particular, they must be made usually in writing, voluntarily and in full awareness of all circumstances described in the best possible manner.

[6] Available at http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last accessed on 12 April 2016).
After the privacy shield entered into force, this will also have to be taken into account. A guide to the EU-U.S. privacy shield can be found at http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf

[7] Cf. for details, Bräutigam/Klindt, NJW 2015, 1137.

4. What are the consequences of breaches of data protection law?

Breaches of data protection law constitute a major risk. The above-mentioned data protection supervisory authorities may not only impose administrative orders, but they also have the option to levy fines up to € 300,000 for each incident (that sanctions will be tightened significantly as of 2018 is addressed in the introduction).

In the individual case a breach (with the intent to make a profit or cause damage) may even be subject to prosecution under penal law. The Act provides in this respect for prison sentences up to two years or a fine for certain serious breaches.

Data protection breaches may lead to fines, claims for damages, compensation for pain and suffering and injunction suits, in severe cases even penal law will be applicable. In any case, they will lead to a loss of goodwill.

And there are also the claims of the data subjects. They do not only have the right to information about the relevant data, they may also demand that these be blocked, deleted or corrected if data are incorrect or must no longer be stored.

Furthermore, there are claims for damage and pain and suffering based on data protection breaches. In February 2016, consumer associations were given the right to institute class-action suits against data protection breaches.

In particular cases, data protection breaches may also qualify as anti-competitive practices and pursued accordingly.

Irrespective of the above, the company will suffer substantial loss of goodwill when a data leak occurs.

5. How can the company minimise such risks?

Companies can and should minimise such risks wherever possible. The first step is to create awareness for data protection. A company must be aware of the fact that personal data are not any given asset they can treat as it sees fit, but personal data must be protected in many ways and are subject to a complex legal network.
If it is impracticable to avoid the processing of personal data (e.g. through depersonalising), the company must have the tools and processes in place that ensure that data processing happens in a lawful way.

Creating awareness for data protection issues and obtaining information are the first steps to minimise risk.

To do so, a data protection management scheme may be suitable, depending on the extent and complexity of the data processing. By issuing relevant policies and maintaining a data protection structure, having competent staff, a data protection officer and if appropriate external consultants and conducting own audits, the company can ensure compliance in this field of law that has such an impact on Industrie 4.0.

5.1 Questions to be answered

In a further step, the company may ask itself the following questions:

- Are personal data collected in a specific Industrie 4.0 project (see also No. 3.1.2 above)?
- Is the collection necessary or can it be depersonalised by removing reference to persons?

This first step can be approached and implemented methodologically, depending on the size of the company, the industry sector and the specific Industrie 4.0 project: To the extent that the necessary capacities are available in the legal department, they should by all means be included. If there is already an external data protection officer, this person should be, from the earliest possible date, involved in these questions and be kept up to date about the Industrie 4.0 matters systematically (e.g. as a part of quality assurance). During this early stage, the inclusion of data protection expertise can help to identify personal references that may at first sight be quite difficult to see (and which might already exist when a reference to a specific individual can be made to a certain date, as in the contentious case of IP addresses) and take them into account in the subsequent deliberations for each project phase.

5.2 Clarify personal reference and/or identification potential

If no systematic inclusion of data protection expertise is possible or desirable, the decision maker must make a conscientious decision as to what information the Industrie 4.0 project should use. If this concerns data that (if only indirectly) allows to draw conclusions regarding e.g. the behaviour or characteristics of individuals, it must be checked whether it is possible to carry out the project without using such data. In this respect, depersonalisation of data might be a solution. Yet, also in this case, utmost prudence is key, because the Act assumes in Sec. 3 No. 6 that rendering anonymous is only deemed to exist in the case of a modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual. If depersonalisation then results in an environment where

subsequent use of data is no longer subject to data protection law, it will also be necessary to change the data in such a way that it is no longer possible to re-establish a connection to the data subject. This means that every variant according to which the reference is still possible, yet with disproportionate expenditure, does not in all cases result in a viable processing authorisation.[8] As a matter of principle, the law regards depersonalisation only as a second step (i.e. as processing of existing data). The initial collection of personal data is hence still subject to a valid justification.

When data are depersonalised in order to create a lawful environment for the subsequent processing, this requires that the individual indications regarding personal and factual circumstances can, in no way whatsoever, be attributed to an identified or identifiable individual. Also in this case, the collection of data (i.e. the step prior to the depersonalisation) requires a valid justification.

5.3 Ways to establish procedures for permitted processing of personal data

If it has been established that the Industrie 4.0 project cannot be implemented without processing personal data, it must be checked whether doing so is admissible or whether admissibility can be established by obtaining consent. As described above, data processing is admissible if either the data subject's consent or a statutory basis is available. The relevant sections of the Act with respect to Industrie 4.0 applications are in particular Sec. 28 and Sec. 32. Sec. 28 of the Act allows, to a certain extent, the collection and storage of data for own business purposes. As a rule, this right is strictly limited to the extent necessary to enter into, implement or terminate a contract. Furthermore, the processing purposes must be laid down and specified right from the start. A typical type of Industrie 4.0 processing, where a large range of often not pre-determinable purposes and added values are at stake, is therefore often excluded from such right. Whether data processing in an Industrie 4.0 application may be based on Sec. 28 of the Act can only be determined upon individual assessment of the case.

With a view to employment relationships, the Act allows the processing of personal data of members of staff to some extent pursuant to Sec. 32. Yet this also means that the admissibility of processing data in an Industrie 4.0 context is limited, e. g. with respect to employee productivity, because the processing is only permitted for requirements regarding the implementation of the employment relationship.

Even if in the individual case further statutory bases may apply to processing (e. g. under the Fiscal Code, the Commercial Code, the codes of social law or the Telemedia Act), there will be many more cases were only consent will serve as sufficient basis for data processing in the Industrie 4.0 context. If, however, a statutory basis is to be applied, this should be ideally documented in writing, e. g. in the procedure register.

Many Industrie 4.0 applications will command that the data subject's consent is obtained if their personal data are to be processed.

[8] Cf. Buchner, in: Taeger/Gabel (Hrsg.), BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2013, § 3 Rn. 44.

Pursuant to Sec. 4(a) of the Act, consent is effective only when based on the data subject's free decision. Data subjects shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent. Even in normal cases (and to the extent that e. g. no special conditions apply pursuant to the Telemedia Act or other conditions based on particular circumstances) consent must be given in writing. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance.

In addition to the elements "legal basis" or "consent" other requirements must be fulfilled to ensure that data processing in the Industrie 4.0 project is actually lawful. Here, the provisions of Sec. 9 of the Act are particularly relevant. They provide that the company must take technological and organisational measures to ensure information security when processing personal data. Specifically, the measures (as described in Annex 9 to the Act) must be taken that are suitable

1. to prevent unauthorised persons from gaining access to data processing systems for processing or using personal data (physical access control);

2. to prevent data processing systems from being used without authorisation (logical access control);

3. to ensure that persons authorised to use a data processing system have access only to those data they are authorised to access, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording (data access control);

4. to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to verify and determine which bodies are to be transferred personal data using data transmission facilities (disclosure control);

5. to ensure that it is subsequently possible to verify and determine whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control).

One measure in accordance with Nos. 2 to 4 is in particular the use of the latest encryption procedures.

Where personal data are processed, the internal organisation of enterprises is to be such that it meets the specific requirements of data protection (e. g. through encryption and access control).

To safeguard data protection in the Industrie 4.0 context is hence no easy task, yet the existing risks can be effectively hedged when the above questions and options are taken into account. In addition the company may conduct a small self-audit in accordance with the checklist on page 20 and then assess how well existing risks are addressed in general, out of the context of individual projects.

6. Where to obtain additional information and support?

For data protection questions, the VDMA offers its members a service desk where they can obtain first information on data protection, e. g. through naming external data protection experts.

Contact person:
RA Daniel van Geerenstein, LL.M.
VDMA Legal Services
Phone +49 69 6603-1359
Email daniel.vangeerenstein@vdma.org

Furthermore, the Federal and State data protection authorities offer information services and model forms (e. g. for the appointment of a data protection officer) on their websites.[9]

The Federal Data Protection Officer also publishes a data protection Wiki with numerous useful references and information.[10]

Information and forms are available e. g. from the GDD e.V., the Association for Data Protection and Data Security.[11]

For complex legal questions, it is possible to obtain external advice from e. g. specialist law firms.

In many cases the model forms and information materials mentioned below will be useful advice to help to solve data-protection issues and reduce the expenditure to tackle data-protection questions.

[9] http://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html (last accessed on 12 April 2016).
[10] https://www.bfdi.bund.de/bfdi_wiki/index.php/Hauptseite (last accessed on 12 April 2016).
[11] https://www.gdd.de/ (last accessed on 12 April 2016).

Further information

Model documents and information materials (in German only, unless indicated otherwise)	
German Federal Data Protection Act – Text and supplementary information (Federal Officer for Data Protection and Freedom of Information)	**http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1.pdf?__blob=publicationFile&v=12**
Information brochure "Die Datenschutzbeauftragten in Behörde und Betrieb" (Federal Officer for Data Protection and Freedom of Information)	**http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO4.pdf?__blob=publicationFile&v=6**
GDD Checklist to assess own knowledge for data protection officers in corporate organisations	**https://www.gdd.de/seminare/Checkliste%20zur%20Fachkunde.pdf**
German language model regarding contract data processing and documentation of results from ADV control measures by the GDD	**https://www.gdd.de/links/downloads/deutschsprachiges-muster-zur-auftragsdatenverarbeitung**
English language model regarding contract data processing and documentation of results from ADV control measures by the GDD	**https://www.gdd.de/links/downloads/englischsprachiges-muster-zur-auftragsdatenverarbeitung**
English language EU model contract for the transfer of personal data to third countries	**http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm**
Guidance by the Düsseldorfer Kreis regarding data protection requirements for app developers and app providers	**http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_App.pdf?__blob=publicationFile&v=3**
Guidance by the Düsseldorfer Kreis regarding RFID use in compliance with data protection law	**http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/Orientierungshilfe_RFID.pdf?__blob=publicationFile&v=4**
Guidance by the Düsseldorfer Kreis regarding data protection and data security in projects: Project and actual operation	**http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_Projekt-Produktivbetrieb.pdf?__blob=publicationFile&v=4**
Model text for obligation to comply with data secrecy pursuant to Sec. 5 of the German Federal Data Protection Act, Sec. 88 of the Telecommunications Act and the protection of business secrets (Federal Officer for Data Protection and Freedom of Information)	**http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/VerpflichtungDatengeheimnis2.pdf?__blob=publicationFile&v=4**
Model procedure register by the GDD	**https://www.gdd.de/downloads/materialien/muster/verfahrensverzeichnis.pdf/at_download/file**
Advice regarding the procedure register and the procedure overview by the Bavarian Federal Office for Data Protection Surveillance	**https://www.lda.bayern.de/media/info_verfahrensverzeichnis.pdf**
Model policies and proposed methods by the Federal Office for Security in IT regarding basic IT protection	**https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/muster/musterrichtlinien/musterrichtlinien.html**

7. Checklist / questionnaire – self assessment

Checklist – self assessment

The following questions are meant to provide guidance and promote data protection awareness with a view to minimising risks. Yet, they are no substitute for a professional data-protection assessment, data protection audit or the appointment of a data protection officer.

1. Has the company already appointed a data protection officer?
   - If no, how is the fulfilment of data-protection reporting duties and the assessment of the lawfulness of each processing of personal data ensured?

2. Is there a topical internal and external procedure register?
   - If no, what are the departments and processes in the company where personal data are processed?

3. Are there written contract data processing agreements in place with suppliers, business partners and affiliated group companies that receive or may access personal data?
   - If yes, how and when are the contract data processors controlled? Are there assessment reports?

4. Have all staff in the company declared their commitment pursuant to Sec. 5 of the Act?

5. How are members of staff trained with respect to data protection?

6. Do the company website and all the apps contain updated data protection declarations and are pertaining data processing procedures based on valid consent declarations?
   - If yes, how is it ensured that the consent declarations are valid, also taking into account how they are actually implemented on the website?

Project partners / responsible editors & legal

VDMA
Legal Services
RA Daniel van Geerenstein, LL.M.
(CESL Beijing / Hamburg)
Lyoner Str. 18 60528 Frankfurt am Main
Email daniel.vangeerenstein@vdma.org
Web www.vdma.org/recht

GvW Graf von Westphalen
Rechtsanwälte Steuerberater
Partnerschaft mbB
RA Stephan Menzemer
Ulmenstr. 23–25
60325 Frankfurt am Main
Email s.menzemer@gvw.com
Web www.gvw.com

Design and Layout
VDMA Verlag GmbH

Year of publication
2016

Photo credits
Title: fotogestoeber – Fotolia.com
Page 3: VDMA

VDMA
Legal Services
Lyoner Str. 18
60528 Frankfurt am Main
RA Daniel van Geerenstein, LL.M.
Phone +49 69 6603-1359
Fax +49 69 6603-2359
E-Mail daniel.vangeerenstein@vdma.org
Internet www.vdma.org/recht

GvW Graf von Westphalen
Rechtsanwälte Steuerberater
Partnerschaft mbB
Ulmenstr. 23–25
60325 Frankfurt am Main
RA Stephan Menzemer
Phone +49 69 8008519-0
Fax +49 69 8008519-99
E-Mail s.menzemer@gvw.com
Internet www.gvw.com

www.vdma.org/recht