PRIVAZYPLAN®

Practical guide for data protection.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION
ON COURSE.

All obligations.
All explained.
All according to plan.

by SecureDataService
Nicholas Vollmer

by
SecureDataService
Nicholas Vollmer

February 2018

Table of contents

... a detailed list of contents can be found on page 367.

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklist for a quick start into the topic can be found on page 225.

Author:
SecureDataService, Nicholas Vollmer, B.A. Engineering
Priorstrasse 63, 41189 Mönchengladbach, Deutschland
Tel: +49 2166 96523-38, Fax: +49 2166 96523-39,
Email: n.vollmer@privazyplan.eu

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

1.1 Foreword to the current edition

Dear Readers,

As author of the PrivazyPlan®, I would like to welcome you to the current edition February 2018. What are the most important changes this month?

- **Data protection in works councils**
  How can it be ensured that a works council also meets the approx. 50 obligations when it comes to their data processing? Who monitors this? We will name the specific challenges faced. Page 14

- **What is a "data protection violation"?**
  What constitutes a "data protection violation" within the meaning of Article 4 No. 12? This question is key when it comes to meeting the documentation and reporting obligations. Page 132

- **Change in the order of obligations in the "master data list"**
  The "master data list of a data processing operation" is where the approx. 40 obligations of each data processing operation are handled.
  For a fluent workflow, it is recommended to first create the record of processing while simultaneously describing the transparency obligations wherever possible. If this approach is taken, the remaining obligations of a particular processing operation can be handled considerably more smoothly. Page 263 [1]

- **"Balancing of interests" has been specified more closely**
  Whenever the legal basis of a processing operation is founded upon "legitimate interests", these interests of the data subjects must be weighed up. Specific examples for the respective interests have now been mentioned. Page 286

- **VdS 10010: a guide for the data protection management system**
  In December 2017, the VdS published a 32-page guide providing companies with a detailed checklist to enable them to systematically tackle data protection. This document is well worth reading. Here in the PrivazyPlan®, the specific chapters are referenced in over 20 places. Page 291 :

- **Is encrypted data considered personal?**
  This important technical query is still unclarified. The various philosophies of the "relative" and "absolute" approaches are explained and the impact of both approaches in practice are also demonstrated. Page 329

- **Changes to PrivazyPlan.zip**
  Various texts and tables are provided as part of the "mini data protection management system" (page 26). New for this month:
  (a) A new table sheet has been added right at the end of "PrivazyPlan.xls": "Transparency text(s)". This explains why the "common transparency notice" is so worth while.
  (b) In sub-directory \GVO_032\ there is a new file: "2017 12 14 ISA+ Blanko.docx". Here you will find a specific template if you are intending to work using the ISA+ security analysis. This will enable you to get your information security management system (ISMS) up and running very quickly.

You will also find key changes from January 2018 on pages 68, 199, 261 and 262. The EU general data protection regulation comes into force in **4 months**! The **25th May 2018** is fast approaching...

I wish you the best of success.

P.S. There is a total of 37 updated sections of text in this edition. You can find all these sections by searching for "New in January" or "New in February".

[1] The following applies to companies managed via DSB-MIT-SYSTEM®: The DSB-Reporter® software enables the "common transparency notice" to now also be used to illustrate these transparency obligations (amongst other aspects). The issue of personal rights (and other aspects) is now also broached in the online report form.

1.2 General foreword

Dear Readers,

As author of the PrivazyPlan® I would like to welcome you to this edition.

To begin with, please allow me some introductory – and personal – observations regarding the EU General Data Protection Regulation (**GDPR**).

How time flies. In January **2011** in Brussels, the EU vice president (Viviane Reding) presented the Commission's draft of a general data protection regulation. Since then, I have followed the subject very closely and reported on it monthly in the TOM-Guide® (see here). In the spring of **2012**, Jan Philipp Albrecht, as rapporteur of the European Parliament on the issue, became very closely involved and effected a great deal. Following turbulent negotiations between the EU Commission, European Parliament and the EU Council, it looked for a long time as though the GDPR would never materialise. But then in April **2016**, totally unexpectedly, it finally happened: Europe has a new data protection law. It will come into compulsory legal effect after a short transitional period of 24 months.

For many data protection officers (myself included) this came as a **"shock"**. We had developed a comfortable familiarity with the German Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) and nobody would ever have thought that it might one day be summarily shredded. After 12 years as data protection officer in my day job, things have suddenly become more exciting again.

As early as June 2016 I set up the website www.privacy-regulation.eu so that I (and my clients) would at least have access to the original regulation document. In the event, it turned out to be very helpful.

Essentially, a proper expert analysis was only possible once the first academic commentary appeared on the market in November 2016 (see here). From that point on, the first detailed expert articles also started appearing in the academic press.

For German legal practitioners, the second "shock" was the substantially **revised German Data Protection Act** (amended BDSG) of April 2017. There too, no result had initially seemed likely from the endless consultations. But all of a sudden, a covert raid under cover of darkness presented us with the new BDSG. www.bdsg2018.de And so everything became more complicated...

As a result, we as data protection officers now have to contend with two (sorry!) "cobbled together" regulatory instruments of inimitable complexity that now extend to 85 instead of the previous 36 pages And our clients have hardly a year to implement the change-over.

In February 2017 I began breaking down the GDPR into the individual obligations it imposes. That was when the PrivazyPlan® was born. The approx. 50 obligations will be identified and explained over the coming ten months and you will be provided with guidance. Over the 350-plus pages of this document I have done my best to put together a practical guide to the legislation.

The next two years will be very interesting because we can expect a lot to happen. It is possible that the ePrivacy Regulation may become law before 25/05/2018 (see page 196). And, hopefully, the supervisory authorities will provide us with clear check-lists and contract templates. To that extent, there is guaranteed to be plenty to do for the monthly PrivazyPlan® updates.

The ideal place to start your exploration of the GDPR and the PrivazyPlan® can be found on page 225.

So for now, in December 2017, I wish you pleasant reading and every success in your endeavours.

1.3 Guidance notes on using the PDF document

Introduction

Before you get your teeth into the technical part of the PrivazyPlan®, we would like to draw your attention to how to get the best out of using this PDF document.

1.3.1 Monthly updates

This PDF document is updated every month and sent out to all authorised subscribers. That process has proved its value as a way of keeping all readers up to date with the latest developments; our data protection manual TOM-Guide® has been kept up to date in that way since 2005. Here are some useful points regarding the updates:

- The **foreword** to each edition (see page 5) explicitly points out the most important new developments. A short explanation then provides more detail. From the foreword you can jump directly to the new content.

- Changes are **highlighted** in yellow. Thanks to the full text search facility in any PDF reader, you can find any change with a simple mouse-click. There are two approaches taken for highlighting:
  - Extensive text modifications are highlighted as follows: "New in May: …" and "Back to the foreword".
  - Small changes are completely coloured-in and look like this: "New in May: Lorem Ipsum dolor sit".

- **Hard copy print-outs become outdated** very quickly. Remember: If you print out the PrivazyPlan®, it may well be out of date in just one month's time. New content may have been added or the existing text changed. Section and page numbers may change. So do not spend too much effort on hand-written annotations to the printed document.

We chose **landscape orientation** for the PrivazyPlan® because we assume that the majority of readers will read the document on a computer screen. Particularly because of the monthly updates, a paper print-out simply does not make sense in the long term.

If your paper print-out is missing text at the top margin, you can scale its size down to 99% in the PDF reader. This will not alter the text's legibility.

1.3.2 Navigation aids in the PDF document

Comprising over 330 pages, the PrivazyPlan® is undoubtedly a sizable document. So how can you keep everything on a manageable scale? Here are our tips for doing so:

- The document contains **bookmarks**. Simply open the bookmarks pane in your PDF reader. As you will see, it makes navigation very easy.

- There are numerous **contents lists** in the PrivazyPlan® to make finding your way around easier. You can move around from one section to another with just a few mouse-clicks. We have taken a lot of trouble to try and make sure the document is easy to use.

- You will find helpful **page references** throughout the document (e.g. "See page 7"). The page references are always clickable so that you can jump straight to the page concerned. We have also highlighted the page references in blue to remind you that they are clickable.
  ⚠ But how do you get back to the place where you clicked on the page reference? Quite easily: just use the key combination "ALT + ⇦" to go back. Try it out. Courtesy of this little trick you can hop back and forth to your heart's content without losing your thread.
  Clicking on the blue page numbers works better in some PDF readers than others and we have no influence over this. Experience has shown that web browsers with a built-in PDF reader create the most issues of all; as such, we recommend downloading the PrivazyPlan® and viewing it with a "real" reader.

- And, of course, there is a full text **search** facility as well. Pressing CTRL+F in the PDF reader opens the Search box. In the Foxit PDF Reader you can even view a list of matches and so quickly select the ones you want.

1.3.3 Amended in German Federal Data Protection Act as of 25/05/2018

In Germany, an amended Federal Data Protection Act applies as of 25/05/2018.

The GDPR is extensive and complicated enough on its own. But as if that were not enough, the GDPR provides roughly 80 opening clauses for national legislators (see page 348).

The German Bundestag made extensive use of those legislative opportunities in April 2017. As a result, numerous obligations arise for the person responsible arise, as set out in **Section 10** starting on page 200. There are also more details in the foreword to Section **10** on page 201.

Here in the PrivazyPlan® the relevant sections are marked by the German flag:
.

The data protection legislation of other EU countries is not incorporated in the PrivazyPlan®.

1.3.4 What is the significance of the references to the TOM-Guide®?

Alongside the PrivazyPlan® there is another expert guide by the same author: the TOM-Guide®.

The TOM-Guide® is a practical data protection manual extending to roughly 700 pages. It provides practical guidance on many aspects of data protection.

At present the TOM-Guide® is only available to a closed group of readers (namely, those companies that are supported by external data protection officers as part of the DSB÷MIT÷SYSTEM®).

Here in the PrivazyPlan®, there are a few dozen instances where reference is made to specific sections of the TOM-Guide®. The topics concerned are dealt with in more depth there. However, the information provided there it is not absolutely essential for an understanding of the PrivazyPlan®.

1.3.5 ... so much information in the PrivazyPlan® and yet there are still unanswered questions...

Despite the not inconsiderable size of the document at over 330 pages, it is not possible for the PrivazyPlan® to describe the roughly 50 obligations imposed by the GDPR in exhaustive detail. Why is that?

The fine details of data protection are extremely complicated. By breaking down the GDPR into around 50 obligations, we have substantially reduced its complexity. In addition, we have explicitly restricted ourselves to its application in the private sector (and therefore ignored the public sector). Nevertheless, it still remains difficult when dealing with the precise details.

Why is the GDPR so complicated?

- The GDPR is **not a harmonised and fully developed set of regulations**. Between January 2011 and April 2016, the EU Commission, the European Parliament and the Council were engaged in tough negotiations. Each of those bodies has its own quite separate interests. The Parliament alone still had over 4,000 outstanding applications for amendments right up to the end. But for political reasons, the document had to be adopted in May 2017. So it was simply tied up and packaged as it was. That comes out of the document in many places.

- The German **translation is not always particularly well composed**. On careful reading there are contradictions and imprecise formulations. We draw attention to them in the relevant places (see page 305). Where there are obvious mistranslations and spelling mistakes we have corrected (and highlighted) them on www.privacy-regulation.eu.

- Many important **key terms** have not been defined in the GDPR. The list of defined terms in Article 4 should have been at least three times as long. As a result, data protection experts are having to deal with a large number of uncertain legal concepts (see Wikipedia). Sometimes it is enough to make you despair.

- In many places, the **sentence construction** in the GDPR is ambiguous. For example, in the case of Article 39 (1b), experts argue as to whether to data protection officer should conduct or merely oversee the staff training. Such arguments could have been avoided if the wording of the regulations had

been clearly formulated. Sometimes a glance at the English original can help make the meaning clearer.

The new Federal Data Protection Act applicable in Germany is in many cases much, much more complicated in its wording. Sometimes grotesquely so. The same is true of the associated legislative justification.

- The roughly 80 **opening clauses** further increase the complexity (see page 348). As if the GDPR did not already have enough rules, exceptions and counter-exceptions, there is a whole raft of counter-rules with their own exceptions and counter-exceptions Wherever the German flag comes into play, application in Germany becomes even more complicated.

- Let us not forget: **data protection is a legal – and therefore difficult – issue.** Essentially, that is quite simply because two quite contradictory interests are at play: **(a)** the interest on the part of businesses to be able to process as much data in as many ways as possible and **(b)** the interest on the part of the data subject concerned in self-determination and privacy,
They are the proverbial "chalk and cheese" that have to be reconciled with one another. That requires a set of rules. And they are complicated.

- The GDPR **seems somehow excessive**. The fines appear to be too high, the record-keeping obligations too extensive, and data transfer to third countries too fastidiously regulated. Why is that? It may be that European businesses have US giants such as facebook, Google, etc. to thank for that.
Sometimes the GDPR reads like a "**lex facebook**". Many of the regulations are manifestly tailored to suit such Internet behemoths. The problem with that is that everyone else has to follow the same rules.

- The **compliance disease** has now spread to data protection as well. It is no longer sufficient for a business "simply to comply with the law". No, that compliance must now be verifiable. For the businesses concerned, that is a disaster. There are more and more rules and following them is increasingly complicated and costly. To such an extent that the core business starts to suffer.

In that regard, data protection is no exception (any longer). Unfortunately. Our aim with the PrivazyPlan® is to help you quickly get back to concentrating on your core business again.

- As at August 2017, there is so far **no generally accepted opinion** on key questions of central importance. It will be some years yet before experts, supervisory authorities and courts are unanimous. Until then, there will be much wrangling around "correct" interpretations. That increases the complexity of the subject because divergent opinions have to be taken into account.

- Overall, we have established that there are at least **two follow-up questions** to every answer. There is simply no end to it all. Virtually every question has several dependent issues and/or multiple possible interpretations. The deeper you delve into a matter, the more you become lost in complicated details that make a simple answer impossible.

For those reasons, the PrivazyPlan® cannot offer a simple solution in some cases. As much as the author regrets the fact.

It remains indispensable for businesses to develop the necessary expert knowledge themselves. That is why we have provided detailed **bibliographical references** in Section 13.3 starting on page 305.

And by the way: even as the author of the PrivazyPlan® one can sometimes be left puzzled. As a reader, you can recognise such occasions by the red bomb symbol: . When you see that symbol it means there are quite clearly contradictory interpretation possibilities. You can find a summary on page 373. We are working on eliminating those technical uncertainties as quickly as possible.

1.4 How does the PrivazyPlan® work?

Introduction

The PrivazyPlan® is a practical guide to data protection under the GDPR. We set out the basic ideas below:

To be clear from the outset: ultimately it is all about **compliance**. We go into that aspect in great detail on page 295 (with a brief summary on page 302).

The ideal place to start your exploration of the GDPR and the PrivazyPlan® can be found on page 225.

1.4.1 Obtaining an overall view of the PrivazyPlan® (Step 1)

So, to begin with, you want to get a general view of the data protection obligations according to the PrivazyPlan®? In that case, you should take a look through the extensive Appendix. We recommend that you proceed as follows:

⚠ Print out the following pages of the Appendix:

- the list of data processing examples starting on page 258
- the brief summary of all obligations starting on page 354
- the detailed table of contents starting on page 367
- the full table of obligations starting on page 370
- the index starting on page 378

... and keep those print-outs in easy reach.

Normally we would not necessarily recommend printing out parts of the PrivazyPlan® because it constantly changes as a result of the monthly updates. But the sections referred to above are simply very important in terms of gaining an overall conception.

1.4.2 Obtaining an overall view of data protection (Step 2)

Presumably, you would first like to know where the basic legal text can be found.

Throughout the PrivazyPlan® we make reference to the websites mentioned below so that access to the original wording is only ever a click away.

It is well worth adding the following URLs to the favourites in your web browser.

a) The EU General Data Protection Regulation (GDPR)

Brussels has provided the **GDPR** in the form of a plain text file. The 99 articles and 173 recitals are written out completely unformatted. There are neither cross-references nor a list of contents.

➔ You can find a readable version with cross-references and much more at www.privacy-regulation.eu/en.

➔ Or go to www.privacy-regulation.eu/dsgvo-privatwirtschaft.pdf for a PDF version that has been abridged for the needs of the private sector.

We are particularly proud of the "**dossier**" function on http://www.privacy-regulation.eu/en/dossier_compliance_demo.htm. We have provided headings for important key statements that you can access via the dossiers. Consequently, all relevant regulation wording is presented in distilled form. That enables you to obtain an overall view of the regulation. Try it out by clicking on the following link: "Data protection officer" dossier. We refer to those dossiers in many places in the PrivazyPlan®.

b) The new German Data Protection Act (amended BDSG)

In Germany, a "new" Federal Data Protection Act applies as of 25/05/2018. Berlin has made the Act available in the form of an extremely impenetrable omnibus act in the *Bundesgesetzblatt* (Federal Law Gazette). Spread over 36 pages there is a mixture of various acts with apparently similar content. Of those, only 13 pages are relevant to the private sector.

➔ You can find the relevant clauses for the private sector at www.bdsg2018.de/de.

➔ Or go to www.bdsg2018.de/bdsg-neu-privatwirtschaft.pdf for a PDF version that has been abridged for the needs of the private sector.

c) The "old" Federal Data Protection Act (old BDSG)

In Germany, the "old" Federal Data Protection Act applies until 25/05/2018. See http://www.gesetze-im-internet.de/englisch_bdsg/index.html. Don't be put off by the date "1990"... it is actually the current version, which was last amended in March 2017.
On the above website you will find links to a PDF version and even an English translation.

But what are the consequences for your business? That is Step 3...

1.4.3 Alignment with obligations (Step 3)

What are most businesses concerned about when aiming to comply with data protection regulations? They want to **avoid fines** (see page 333). Therefore, the PrivazyPlan® breaks down the GDPR (including the amended German Federal Data Protection Act) into obligations relevant to that aim.

a) What are obligations? Where can you find them?

How have we arrived at the term "**obligations**"? The reason can be found in Article 39, which says as much as:

> *"The data protection officer is responsible for the task of instructing on, advising on and overseeing the **obligations of this regulation**."*

In general, all **provisions relevant to the imposition of fines** in Article 83 (4) and Article 83 (5) should be seen as "obligations". On that basis, we have sought out all practically conceivable obligations identifiable by wording such as *"... must ensure..."* or *"... must document..."*.[2]

On page 333 you can find more information on fines, compensation, intervention capabilities of the supervisory authorities, etc.

[2] In Germany, Section 41 BDSG (Amended) ("Application"), Section 42 BDSG (Amended) ("Penalty Regulations") and Section 43 BDSG (Amended) ("Fine Regulations") also apply.

Where are the obligations to be found in the GDPR and the new Federal Data Protection Act? Are they listed in a particular place? No, unfortunately it is not that simple. You have to deduce the obligations yourself from the text.

After a detailed search, we identified about 50 places where obligations arise. The following examples are illustrative:

- Article 5 (2): "The person responsible is responsible for compliance with Paragraph 1 and must be able to **provide evidence** such compliance (accountability)."
- Article 7 (3): "... the person concerned **shall be notified** to that effect prior to providing consent..."
- Article 8 (2): "The person responsible [must] **satisfy himself/herself** that the consent has been given by the person with parental responsibility for the child or with that person's agreement."

So around 50 obligations that a business should not on any account ignore have been identified in that way. It is those obligations that the PrivazyPlan® focusses on.

The identification of obligations is associated with a **degree of uncertainty**. Numerous provisions of the GDPR are not clear on whether a practical obligation might be involved in the case concerned. In at least 21 places in the Regulation, for example, a requirement for "evidence" is stated or at least implied. In more than one instance, the reader could easily interpret this as an obligation to provide evidence.

The PrivazyPlan® offers the dossier "Obligation". In it, the relevant parts of the GDPR are brought together in distilled form. That makes it easier to get a grip on this extensive topic.]

⚠ IMPORTANT NOTE: We have identified the obligations imposed by the GDPR to the best of our knowledge and belief. In the future there may be supervisory authorities that identify additional obligations. To that extent we offer no guarantee

that our list of obligations is complete or correct. However, with the benefit of the monthly updates you would quickly find out about such changes.

b) Every obligation is given a code

Each of the above obligations has a **unique code** such as **[GVO_017a]**. What is the significance of that? What is it used for?

- The **first part of the code** refers to the statutory regulation on which it is based. For example, "GVO" stands for the GDPR. [3]
  In Germany, "BDSG" stands for the new Federal Data Protection Act and "TMG" refers to the German Electronic Media and Communications Act (Telemediengesetz).

- The **second part** of the code refers to the article (and/or paragraph) number. Where an article or paragraph gives rise to more than one obligation, they are numbered alphabetically (e.g. "017**a**").

- The **practical value** of the codes is very high because over time one can learn many codes by heart and thus more easily retain a clear overall view within the PrivazyPlan® documents. When talking to colleagues it can also save a considerable amount of time and confusion if one uses the codes instead of the full description of the obligation. Especially in international businesses, the obligation codes overcome any language barriers.

Thus, the obligation codes are not simply consecutively numbered (1, 2, 3, ...) but rather are based on the article/paragraph number. We decided on that method of numbering because it gets around potential future problems if new obligations are identified. In other words, the present codes will never change. That is fundamentally important.

c) And what about the possible compensation claims?

Apart from the fines, there is also the threat of compensation claims, of course. According to Article 82, persons affected can claim compensation for both financial and non-pecuniary loss or damage.
However, the potential compensation claims are even more difficult circumscribe in the Regulation wording than the risk of fines. In principle, an affected person may claim compensation due to "any" state of affairs.

[3] The obligations of the data protection officer are identifiable by the codes "[DPO_...]", see Section 11 starting on page 221.

Since that can hardly be circumscribed, the PrivazyPlan® initially concentrates only on the risk of fines.

But how can we better understand the obligations and where are the challenges described in detail? That is Step 4...

1.4.4 Making obligations understandable (Step 4)

We explain every single obligation in very practical terms. You will find out:

- what the obligation consists of (summarised in a few sentences)
- whether the Federal Data Protection Act recognised similar obligations
- where the associated provisions regarding fines can be found (see also page 333)
- whether there is specific technical literature on the subject
- whether the new Federal Data Protection Act in Germany will be applicable in the area concerned
- ... and plenty of valuable technical guidance on specific questions of practical significance.

In that regard, **Sections 2 to 10** explain what the obligations mean in practical terms for the person responsible.

In technical terms, the sections referred to above merely scratch the surface of the issues involved, of course. Our aim is to point you towards the **technical literature and information sources** that are an essential prerequisite for a basic understanding of the law (see page 305).

For important issues we also offer **detailed technical information** in Section 13 starting on page 290. There we summarise matters that are very important and cannot be found in such distilled form in any textbook.

But in what order should you tackle the obligations? How do you set your priorities? That is Step 5...

1.4.5 Setting priorities (Step 5)

The roughly 50 obligations are not firmly prioritised in relation to one another. To that extent, the controller has entirely free rein in setting their personal priorities.

On page 16 we set out in detail how you can go about setting your priorities. We provide you with a Microsoft Excel spreadsheet that you can customise as you see fit.

But how precisely are they to be transformed into company practice? That is Step 6...

1.4.6 Organising and implementing obligation compliance (Step 6)

In **Sections 2 to 10** we also explain how the person responsible can satisfy the obligations in practical terms.

Since, as we know, we are aiming at a **compliance management system** (see page 295), conformity with each obligation should initially be organised by applying the "PLAN, DO, CHECK, ACT" process.

Therefore, the PrivazyPlan® sets out precisely those four steps for every single obligation:

- **PLAN:** How does the company intend to meet the obligation in each case? What is the self-expectation here? What priority is accorded? Who is responsible? Whose job is it? How is "successful" compliance with the obligation measured? How often is it to be checked? General guidance on the "plan" step can be found on page 20.

- **DO:** What precisely does practical implementation of the obligation concerned look like? Are there job instructions and/or a check-list for the task? Continuously updated documentation records the degree of obligation compliance. General guidance on the "do" step can be found on page 22.

- **CHECK:** This step involves checking compliance with the obligation concerned at the time intervals previously defined. The process is documented in writing. Have deficiencies in obligation compliance been identified? General guidance on the "check" step can be found on page 23.

- **ACT:** If there are deficiencies in compliance with the obligation concerned, the employee responsible in each case must be notified. He/she then decides whether action is required. Where necessary, the plans should be revised. General guidance on the "act" step can be found on page 23.

The PrivazyPlan® aims to outline the above steps for every one of the roughly 50 obligations. That means that your business can start immediately with the practicalities.

Presumably, it will primarily be the "DO" step that presents the business with the greatest challenges in terms of time and scope.

There are numerous **sample forms** in **Section 12** on page 223. They provide precise ideas on how some of the obligations can be satisfied.

1.4.7 … and what about the data protection officer's obligations ?

In **Section 11**, we describe the **eight obligations of the data protection officer** (see pages 215-223).

Those obligations arise from Article 37, Article 38 and Article 39.

The obligation to appoint a data protection officer initially arises from Article 37 (1) and (in simplified terms) only affects those companies whose **core activity** by its nature or scope impinges particularly on the rights and freedoms of the affected persons.

In Germany, there is an obligation under Section 38 of the amended BDSG to appoint a data protection officer if at least **ten persons** are constantly engaged in automated data processing (e.g. have personal e-mail addresses). See page 175.

If you company **does not** (have to) appoint a data protection officer, then somebody in the company must take on those obligations (e.g. in order to act as a contact point for supervisory authorities).

1.5 Important decisions to start with

Introduction

There are a number of quite fundamental decisions that a business has to take. We aim to briefly set out the most important at this point. You will see that these questions are quite complex, so you are not expected to be able to provide the answers right here and now. But keep in mind that the questions will become relevant at some point or other. Your data protection officer will undoubtedly be happy to advise you.

You can, for example, document the results of your considerations in the data protection policy (see page 228).

1.5.1 Which compliance management system best suits you?

As we know, data protection is a **compliance** issue (see page 295).

Make a decision as to how data protection compliance is to be organised at your company. Do you want to create all documents and to-do lists in Microsoft Word and Excel? Or do you want to use a Microsoft Sharepoint server, perhaps, so that you can keep the plethora of information easily at hand? Or maybe you prefer to purchase a costly professional software solution.

So how high up your list should compliance be placed? How "professional" do you want the results to be? Every business has to find the solution that best suits it here. You can find explanatory considerations in the section "Compliance" on page 295.

In what way is the data protection officer supposed to supervise performance of the obligation In the meaning of Article 37? In what precise way is (read) access to the documents and evidence supposed to be granted? There are a number of options, such as: (a) by exchanging data via email or (b) by access of the DPO to the company network via remote desktop or VM ware, or (c) by access to a cloud-based sharepoint server?

➔ The file „**PrivazyPlan.zip**" contains what's necessary for a minimal data protection management system (see page 26).

1.5.2 What about the works council/data protection officer/medical officer?

Those "company roles" also store and use personal data. Nevertheless, the practicalities of data protection for those roles tended to be a bit of a blank area on the data protection map as the board was concerned.

In particular, the monitoring of data protection measures in the works council has not been afforded much attention or supervision up to now (not least as a result of a judicial ruling in Germany in 1997 in which the company data protection officer was refused authority to monitor the works council).
Data processing by the works council and its cooperation with the data protection officer is described in Section 3.11.4 of the TOM-Guide®. New in February: The issue of processing data relating to the "Representation of interests of employees" is broached in Section 26 para. 1 sentence 1 clause 2 Amended BDSG. The periodical RDV 06/2017 reports in detail on pages 279-284 on the data protection responsibility with respect to the works council (but without tangible results).

Put in writing how with respect to the works council processing operations **(a)** personal rights are garanteed (see pages 29-79), **(b)** who the data protection contact person for employees is, **(c)** how it is ensured the works council possesses the required specialist knowledge, **(d)** how the proof of compliance with the basic principles is documented, **(e)** who monitors compliance with data protection in the works council, **(f)** who creates the record of processing and (where applicable) the "common transparency notice" (see page 90), **(g)** to what extent the works council meets its control obligation with respect to Section 80 BetrVG and evidences this, **(h)** how the legality and fairness of processing operations are ensured, **(i)** how information security is continually ensured and documented, **(j)** how any data protection breaches are documented/reported, **(k)** how the works council members are guided within the meaning of Article 32 (4), **(l)** whether any commissioned data processing operations are contractually drafted in a correct manner, **(m)** how the role of the data protection officer is realised.
Back to the foreword

Make a decision as to the nature of data protection on the part of the works council/data protection officer/medical officer under the GDPR as of 25/05/2018.[4]

In view of the threat of fines and claims for compensation (including non-pecuniary loss) (see page 333), the aim should be try to eliminate any blank areas under the GDPR as of 25/05/2018. The board should decide how to deal with them.

1.5.3 Is encrypted data subject to the GDPR?

One of the most fundamental questions of data protection is whether **encrypted** data is subject to data protection and, therefore, the provisions of the GDPR.

That crucially important question is examined in Section 13.9 on page 328.

Make a decision on whether you agree that encrypted data is subject to data protection.

In the sections referred to above you can find guidance on the things that the decision may affect. That should be reflected in the way the roughly 50 obligations are actioned.

1.5.4 To what extent does the GDPR apply to paper-based documents?

There is unfortunately a large legal grey area with regard to unsystematic paper-based data. Does the GDPR apply in its fully scope? This questions is explained on page 350 .

1.5.5 Common transparency notices

Numerous passages of the GDPR confer a right to information and transparency to the data subjects. This affects a number of different obligations.
For example, the processing of data submitted via a website contact form would require approx. five different notices that are fairly similar.
It is possible to combine all of these notices for each data processing operation. This would save time and hassle. This is described in detail on page 91. Is this the right approach for you?

[4] Issue 07/2017 of the professional magazine ZD addresses this question on page 322, at least as regards the works council.

1.6 Prioritising the obligations

Introduction

Roughly 50 obligations are identified within the PrivazyPlan®. The task of prioritising them should be tackled at as early a stage as possible. If you have appointed a data protection officer, he/she will doubtless assist you (see page 218).

1.6.1 A rough plan for implementing the GDPR

Before beginning with the following points, please make sure you have ready the introduction on page 225 .

You can **start** implementing the GDPR in only four days. The result of each day will be the nomination of a specific person to accept responsibility for the tasks required (highlighted in red in the following). VdS guideline 10010 (see page 291) goes into more depth with respect to these aspects in chapter 4 contained therein ("Organisation").

a) Day 1: Management accepts the challenge

Implementation of the GDPR depends on the resoluteness of a company's management. Data protection can only succeed if the management sets clear priorities and makes the necessary resources available. A brief introduction to data protection compliance can be found on page 302.

➔ Designate a director who will bear the responsibility.

The customary approach in the area of "compliance" is that a company's management initially drafts a **DATA PROTECTION POLICY** and signs the policy in person. Here is where the company's objective with regard to data protection is unmistakably set out and made available to the employees (see page 228). This means the OBJECTIVE has now been defined.

The management team may then be instructed to implement this objective in the company. **This requires, above all, a rough review and PLANNING of the obligations.** The overview of all obligations on page 354 can assist with this review. Management should issue clear instructions to the departments on how the respective obligations can be performed. Doing this in a plan-do-check-act approach means you are on the right track to long-term success.
(In the "mini data protection management system" starting on page 26, this means: for each obligation, a planning text is provided in PrivacyPlan.xls. The departments must gear their action to this planning text.)

The time constraints of employees is already to most critical resource in achieving data protection compliance. A diligently done data protection compliance will cost several hundred working hours. If all existing employees are at full capacity with the existing tasks, new employees (internal/external) would have to be hired.

The Data Protection Officer will advise and instruct the company. He can however not write the work instructions for every single employee; he also cannot conduct the contract negotiations with external service providers. These sorts of issues must be taken care of by the company itself (see page 303).

Data protection compliance is achievable with a clearly defined objective, a well laid-out planning and adequate human resources.

b) Day 2: Data protection officer (and EU representative, if necessary)

Check whether your company is required to appoint a data protection officer (DPO). See obligation **[GVO_037]** on page 174. Please ensure that this person has the full technical expertise from the beginning.

➔ If necessary, designate a data protection officer (DPO).

Chapter "Obligations concerning the data protection officer, etc." starting on page 173 sets out all the details concerning this obligation. The person designated data protection officer must not fill any of the other positions described in this chapter, as otherwise a conflict if interest may arise. All obligations are explained in detail in chapter11 starting on page 215 .

Over the short term, the DPO has to instruct the controller with regard to its obligations under data protection law. See obligation **[GVO_039]** on page 188 (or on page 217). This can be done quickly and reliably with the help of PrivazyPlan®.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

1.9 What does the PrivazyPlan® not do?

Introduction

The PrivazyPlan® is **not** a classic textbook.

A "normal" textbook on the GDPR would generally claim to illuminate every aspect of the entire regulation.

But the PrivazyPlan® only looks at the **obligations backed by the power to impose fines**. That means that only around 30 of the 99 articles of the GDPR are considered in this document. The other articles are (almost) entirely ignored.

All provisions relating to the public sector are excluded. The PrivazyPlan® is thus quite specifically only aimed at private-sector businesses.

New in February: The PrivazyPlan® is not a certifiable data protection management system. It may explain the data protection obligations and provide checklists, but it does not constitute a complete guide for internal company organisation. Reference is made, for example, to VdS guideline 10010, which provides information on this aspect.

Further **technical information** is of course also needed for overall understanding. Numerous sources are described in detail in section 13 starting on page 290 .

A comprehensive collection of specialist literature and online sources is available starting on page 305.

1.10 Data protection management system with minimal resources ("mini-DSMS")

Introduction

You would like to implement a data protection management system ("DPMS") in your company? Highly specialised software products that do exactly that are available (as described on page 300). But it can be done in an even easier way:

➔ Our minimum solution can be found at http://www.privazyplan.eu/PrivazyPlan-Demo.zip

This "mini-DPMS" will enable you to perform all obligations described in PrivazyPlan®. All you need is a spreadsheet software. New in February: Together with VdS guideline 10010 (see page 291), the GDPR can be implemented in practice very successfully.

Our approach is based on three essential ideas:

1. A **sub-folder** is created for each obligation described in PrivazyPlan®. All documents relating to the respective obligation can be deposited here.
2. **Miscellaneous documents** can be saved to the sub-folder "Miscellaneous", provided they are relevant for a number of obligations.
3. The file **PrivazyPlan.xlsx** is among the documents bearing relevance across numerous obligations. This file allows you to work on obligations and document the progress made,

as is explained in the following:

1.10.1 Regarding 1: A sub-folder for each obligation

As you progress, you will be dealing with a large number of documents associated to a specific obligation. These include: Technical literature, work instructions, checklists, attestations, consent declarations and many others.

This is why PrivazyPlan.zip has a separate sub-folder for each obligation. This is also the place to store documents relating to the PDCA cycle, as is explained in the general work instructions on page 20. The forms contained in chapter 12

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

2.0 Introduction

Personal rights

This section describes all the obligations that have to do with the privacy rights of the data subjects; see Chapter III of the GDPR, Articles 12-23.

These obligations are important because the controller has to ensure a large degree of transparency and so the data subjects can very easily complain and even demand compensation.

The aspects of personal rights are also discussed in VdS guideline 10010 (see page 291) in chapter 10.12 found therein (“rights of affected persons”).

Each obligation starts on a new page so that you can print them out separately if required.

2.1 Providing comprehensive information when collecting data [GVO_013]

Personal rights

According to Article 13 (1) and Article 13 (2) the company must inform the data subject in extensive detail right from the point when data is collected. The aim of that is to ensure fairness and transparency of data processing. We could look on that information as a sort of “enclosed leaflet” as provided with medication. [5]

The code assigned to this obligation is **[GVO_013]** (see page 12).

2.1.1 General information on obligation [GVO_013]

The supervisory authority can impose **substantial fines** for contraventions under Article 83 (5b) (see page 333). So, from that point of view, compliance with this obligation is important in order to avert or at least minimise fines (and possibly compensation claims).

The German Data Protection Act (as applicable until 25/05/2018) did not envisage any such obligations. Only in Section 13 Para 1 TMG was there a comparable obligation regarding the duty of instruction on web pages (see obligation **[TMG_013]** on page 198).

The **technical literature** (see page 305) contains a number of helpful documents such as: ● DSK short paper● The 11-page GDD practical guide GDPR VII (“obligations concerning transparency”). ● Trainingseinheit 6 (“rights of affected persons and notification obligations”) of the information series “Fit für die Datenschutz-Grundverordnung”.

2.1.2 What does obligation [GVO_013] mean?

Compared with Section 34 Para 1 BDSG, many more details have to be disclosed; apart from that, the information has to be provided unprompted(!). To that extent, the GDPR is quite immediately obvious to the data subject. Whenever data is to be collected, a long list of details is supplied in advance. There is no such thing as random data collection any more. The data subjects are very well informed right from the outset; therefore, more queries or critical remarks can be expected. In some cases, the controller will have to disclose this or that detail they would actually rather not reveal (because they are worried that persons affected might refuse to allow their data to be processed or could choose not to enter voluntary details).

⚠ An absolute novelty is the detail in Article 13 (1d) that the “legitimate interests” of the controller must be disclosed. Thus the data subject can see quite clearly what the purpose of the data processing is or what the “motivation” for it is. That makes data processing especially “open to attack” because the fact of permission under Article 6 (1f) does not recognise any overriding interests of the data subjects and, accordingly, the data subjects can object under Article 21 (1) (and the data can be restricted under Article 18 (1) until the matter is clarified, see page 60).
Accordingly, the legal basis for data processing should be documented in the record of processing as per Article 30.

Another new feature is the requirement that according to Article 13 (1b) the contact details of the data protection officer are to be provided right from the point of data collection. Thus the “obscurity” of the data protection officer is at an end. It is to be hoped that, as a result, dissatisfied data subjects will first contact the data protection officer before registering a complaint with the supervisory authority.

The subdivision of the notification obligation in Article 13 into Paragraphs 1 and 2 is surprising and is probably due to historical reasons (see Kühling/Buchner in marginal note 20f to Article 13). The controller will not be doing anything wrong if he/she always provides all information referred to in both paragraphs.

Recital 62 makes a restriction that the right to information is superfluous if **(a)** the person already has the information or **(b)** the data processing is explicitly governed by a legal requirement or **(c)** notification is impossible or involves unreasonable expenditure of time and effort.

Tip: it is essential that this obligation to give notification is always met because failure to do so is immediately obvious. Not only the data subjects but also the supervisory authority and your competitors(!) will immediately notice its absence. The risk of fines or compensation claims is high.

[5] Something in the sense of: *“For details of the risks and possible side-effects of this data collection, please contact the company responsible or its data protection officer.”*

2.1.3 How do you comply with obligation [GVO_013]?

As part of the PrivazyPlan® we suggest the following procedure; in it, a separate document is created for each phase of the “Plan-Do-Check-Act” cycle.

Very briefly, it is about the following: ● Obtain the record of processing to identify all data processing operations concerned. ● Prepare the required information notice (as far as it has not already been prepared together with a “transparency” notice, see page 267). ● Make the notices available to the data subjects in a suitable format (i.e. on the website). ● All new/modified data processing operations must be prepared and published as soon as possible.

It goes without saying that all the above points can be adapted to your specific company circumstances.

a) Planning a strategy (“Plan”)

The executive management should first of all consider a fundamental strategy. We provide a number of pointers for doing so below. Only when that has been done should the implementation phase be started (see further on). You can proceed as follows:

- ☐ Follow the general notes on planning on page 20.
- ☐ It is not clearly specified whether the **name of the data protection officer** has be stated explicitly in the information notices. The executive management should decide whether an impersonal e-mail address (such as dataprotection@myCompany.com or dataprivacy@myCompany.com) should be cited or whether the data protection officer should be identified by name (e.g. “Please contact Nicholas Vollmer at N.Vollmer@SecureDataService.de“).
- ☐ There can be **exceptions**. Recital 62 states that the obligation to give notification is superfluous if (a) the data subject already has the information or (b) if storage or disclosure of the information is expressly governed by legal requirements or (c) if notification is impossible or involves unreasonable expenditure of time and effort.
  It is a case of the executive management fundamentally examining and discussing those exceptions. What is Brussels aiming to achieve by those exceptions? Are there obvious scenarios of that type? When can a business save itself the trouble of notification without possibly exposing itself to the risk of a fine (perhaps even as a result of a misunderstanding)?
  If a business dispenses with notification, where are the reasons for doing so documented? Has the executive management explicitly approved the decision?
- ☐ If the data collected (e.g. on a website) is stored, is it also documented what specific information notice was available to the data subject? It would be sufficient to record the relevant document code (e.g. “i001_en”). It would then be possible to prove retrospectively that the person had been informed (and in what way).
- ☐ What can you do if, due to **lack of space** for example, prior notification is not possible? This is the case, for example, with vending machine sales, telephone transactions and prize draw mailshots. In those cases it will be very difficult to provide the required information. A decision has to be made in this connection. Should **QR codes** be offered, for example, so that the person can quickly access the specific information notices on the Internet using a smartphone? Other examples can be found on page 9 of the GDD practical guide GDPR VII.
- ☐ The (information) notices pursuant to obligations **[GVO_013]**, **[GVO_013a]**, **[GVO_014]**, **[GVO_015]** and **[GVO_030]** are identical to the largest extent. It is possible to combine these notices in a SINGLE document. This saves time and repetitions (see page 91). Is this your preferred option? ➔ A sample for this type of standardised documentation can be found on page 267.

b) Implementation (“Do”)

Once the above plans are complete, the obligation can be practically dealt with. Preparatory work is required before the obligation can be implemented:

- ☐ Get hold of the record of processing (as per Article 30 and obligation **[GVO_030]** on page 90). The list will be kept either by your data protection officer or another person with responsibility for it. With the help of that list you will be able to see what the information notices to be produced need to refer to.
  (It might be possible to generate a suitable notice from the record of processing.)

And then do the following for the information notice for every single data processing operation:

☐ Draft the wording of the information notice. If you prefer not to prepare a common transparency notice for obligations **[GVO_013]**, **[GVO_013a]**, **[GVO_014]**, **[GVO_015]** und **[GVO_030]**, you can save the notice i.e. in the mini data protection management system in subfolder \GVO_013 (see page 26); otherwise you can save a common notice in subfolder \GVO_030. According to Recital 39, it has to be easily accessible and understandable and written in clear and simple language.

☐ Find out at what points the data is collected in the case of the data subjects. Is that done online and/or by fax/on paper? It is precisely there that the information notices will subsequently have to be published. That may be (a) on the website in a place directly adjacent to the data entry form, or (b) on paper forms, e.g. in an attachment, or (c) on the telephone by reading out a prepared script.
In the above file, document when and where you have published the notice.

☐ Is this data processing operation subject to a **joint responsibility** pursuant to obligation **[GVO_026]** described on page 149? Then the essential provisions of the underlying contracts must be made available to the data subjects (see page 152). The relevant provision is Article 13 (1a), which requires disclosure of the controller: All controllers would be listed (along with the essential contractual provisions).

Once you have produced and published an information notice for all data processing operations, the “implementation” phase is complete for the time being. Congratulations, you have got the job done!

c) Checking (“Check”)

Compliance with this obligation has to be regularly monitored as of 25/05/2018. The controller for the check can proceed as follows:

☐ Follow the general notes on checking on page 23.

☐ Consider what a relevant check question might be. There are, of course, many different aspects of the information obligation that you could ask about. The following examples are illustrative:
• Are there guidelines or directives for dealing with the obligation to provide information? How do you ensure that the company actively practises this obligations?
• Does the company utilise the possibilities of the GDPR regarding the situations in which notification is superfluous? How is that verifiably justified?
• Does the company have a list of all information notices so that they can be checked selectively for completeness and correctness?
• How does the company ensure that the information notices do not differ from the contents of the record of processing?
• How does the company ensure that the notices can be understood by the data subjects and that they are available in the required local languages?

• How can you prove which information notices were available to the data subjects at the time of data collection?

d) Communicating potential for improvement (“Act”)

If monitoring of the obligation has potential for improvement, that potential must be formulated and reported.

☐ Follow the general notes on the Act phase on page 23.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

3.0 Introduction

Documentation and evidence

The obligations concerning documentation and evidence are particularly important in relation to dealing with the **supervisory authorities**. When conducting audits and checks, the supervisory authorities will request the documents described in this section.

Only in extreme cases does this lead to a fine.

[Provided as part of the PrivazyPlan®, there is a [redacted]". In it, the relevant parts of the GDPR are brought together in distilled form. That makes it easier to get a grip on this extensive topic.]

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

4.0 Introduction

Legality and consent

When is a (data) processing operation permissible? Or when does it excessively interfere with the legitimate rights and freedoms of the data subjects?

This is a frequently complex question. Regrettably, the GDPR does not offer any systematic answer. The controller must rather come up with its own solutions to assess and evidence the question of legality.

There is on particular sentence that should always be remembered:

> "A data processing operation is permissible, if
> (a) it is based on a **law**, **contract** or **consent**,
> (b) it is conducted for **employment** purposes,
> (c) the controller has a legitimate and prevailing **interest**,
> (d) or if there are other legal bases, such as a **works agreement**."

While this sentence is a gross simplification or the facts, it does assist in keeping an orientation.

Why is this sentence a gross simplification? This will briefly be explained in the following:

- A **law** must explicitly **postulate** the respective data processing operation. It must also not contravene the fundamental principles of the GDPR. It must also be assessed, whether such law is not "overridden" by the GDPR, which would render it inapplicable. Not an easy task.

- There has to be **contract** with the data subject. There may however also be contractual claims by third parties, which are difficult to appraise. The contract must not establish an unreasonable link to other performances.

- A **consent declaration** must haven given voluntarily and can be revoked at any time. Consent declarations must be verifiable at all times. Special requirements apply to children. Consent declarations can lapse if they have not been utilised by the controller for an extended time.

- In the case of **employment purposes**, national regulations of the respective country may possibly have to be observed.
  In Germany, this is Section 26 of the amended BDSG.

- The **legitimate interest** of the controller must be considered carefully. It must be able to evidence a balancing of interests. (see page 286). The data subjects may object against it.

- A works agreement can be a walk on the tightrope if the intention is to legitimise a certain data processing operation without falling short of the protection level prescribed by the GDPR.

- Separate provisions of the GDPR apply to particularly "sensitive" data.

All of the above points concern the question about the general lawfulness of a data processing operation. This is examined in the present chapter 4.

There are also other aspects of legality to be considered. This question will be revisited later, in particular with regard to the disclosure of data to third parties (within and outside of the EU/EEA) (see obligation **[GVO_044]** on page 169).

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

9.0 Introduction

Other data protection rules

Article 39 (1a) requires the data protection officer to also instruct and advice the controller with respect to "other data protection rules". This is a far-reaching requirement as will be shown in the following chapter.

For various reasons, the PrivazyPlan® cannot provide a complete list of all existing data protection rules at this point. As a result, each controller must ascertain whether additional obligations need to be complied with.

9.1 European regulations

Other data protection rules

The following EU regulations are of particular interest for non-public bodies in Europe:

9.1.1 EU General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) was adopted in April 2016 and is effective in all member states as of 25 May 2018. The resulting obligations for non-public bodies in Germany are described in detail here in the PrivazyPlan®. Also see page 348.

It is intended for the EU data protection guidelines 94/46/EC from 1995 to govern all data protection in Europe until this time. However, the various methods in which this is being handled in EU member states is causing problems, as described in Recital 9. As a result, this EU directive is being **repealed** in accordance with Article 94.

9.1.2 EU ePrivacy regulation...work in progress

Intensive discussions are underway in Brussels regarding the private sphere in electronic communications.

An ePrivacy regulation (EPR for short) is set to be concluded by 25/05/2018. Many experts have their doubts about this ambitious schedule; however the adoption of GDPR in April 2016 demonstrated what is possible where there is a political will.

A proposal by the EU commission was adopted on 10 January 2017. A proposal by the EU parliament was adopted on 26 October 2017 (also see here and here). New in February: An ePrivacy discussion paper was published on 11/01/2018. Now the EU Council will have to deal with the issue. Then three different EU committees have to come to an agreement.[43]

The Trilog negotiations appear to have started in late November; there seems to be the theoretical possibility, that this regulation takes effect on 25 May 2018. The German Federal Government is sceptical.

The GDPR and the (future) EPR will then govern data protection uniformly and mandatorily across Europe. Europe is a harmonised electronic market. in every respect.

Directive 2002/58/EC from 2002 applied up to now. As with every directive, 2002/58/EC is not immediately effective. Indeed, EU states will need to enact corresponding laws. In Germany, for instance, this takes place via TMG and TKG (see further below.

Once the wording of EPR has been officially decided, it will be published by us at www.eprivacy-regulation.eu.

9.2 National legal regulations in EU member states

Other data protection rules

The GDPR is intended to harmonise data protection across Europe. The heading of the law would not explicitly mention "free movement of data" if this were not the case. However, there are many opening clauses that allow EU countries to make individual amendments (see page 348).

[43]In January 2017, a proposal with translations in all EU languages was published. A new proposal was published in October 2017.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

10.0 Introduction

Amended BDSG

The GDPR is extensive and complicated enough on its own. But as if that were not enough, the GDPR provides roughly 80 opening clauses for national legislators (see page 348).

These opening clauses allow national legislators to specify the data protection requirements and to adapt them to other national laws.

Here in the PrivazyPlan® the relevant sections are marked by the German flag: .

As of August 2018, the technical literature (see page 305) does not include as many helpful documents: ● Data Protection Practices (DatenschutzPraxis) 07/2017, pages 17-19.

The content of this chapter could still be changed. In August 2017, the amended BDSG was still too fresh for final assessments to be made.

10.0.1 The new legislation ("DSAnpUG-EU")

The German Bundestag made extensive use of those legislative opportunities in April 2017. The different design stages of DSAnpUG-EU can be found here. In a number of ways, the result is a very complex "omnibus law", which mystifies even data protection professionals. The official text was published on 05.07.2017 in the Federal Law Gazette.

Article 1 (approx. 75% of Part 1 and Part 2), Article 7 and Article 8 of the Amended BDSG are relevant to the private sector. The scope is approximately 13 pages long, and is therefore 50% of the size of the scope of the old German Federal Data Protection Act (here).

Various ways in which you can access the legislative text can be found in chapter 1.4.2 on page 10.

According to Article 8 of DSAnpUG-EU, the amended BDSG will come into force on 25 May 2018. At the same time, the existing BDSG will expire.

If your company has already appointed a data protection officer in accordance with Section 4f of the old BDSG, page 176 offers a few tips on how this can be dealt with in the future.

➔ The amended BDSG is available at www.bdsg2018.de/de .

An English translation can be seen here.

10.0.2 When will the amended BDSG come into force?

This issue is addressed by Section 1 Para. 4 amended BDSG. This generally applies

1.) for all public bodies in Germany,
2.) when working in **German establishments**,
3.) and the controller is governed by the scope of the GDPR, as described in Article 3.

⚠ This also applies to all companies within the EU/EEA, provided that all personal data is processed in a German establishment.
Because the term "**establishment**" has not been defined, a thorough examination may be necessary in individual cases. Typical questions are: Is it an independent or dependent establishment? Does the establishment have anything to do with the actual processing? If the European Court of Justice's very wide definition of a 'establishment' is to be used (according to which – in very basic terms – a bank account in Germany is sufficient). See Chapter 3.7.6 in the TOM Guide® (in great detail, on five pages).

[A dossier on "establishment" is provided as part of the PrivazyPlan®. In it, the relevant parts of the GDPR are brought together in distilled form. That makes it easier to get a grip on these extensive topics.]

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

11.0 Introduction

Obligations of the DPO

The first prerequisite is that the company has appointed a data protection officer. The related obligations of the controller are important.

➔ See [GVO_037] to [GVO_039b] in Chapter 8 starting on page 173.

11.0.1 What is the data protection officer NOT obliged to do?

There is the question of whether the field of activity of the data protection officer will change, in contrast to the times of the old Data Protection Act. This must clearly be in the affirmative.

The GVO commentary by Gola in marginal notes 2, 4 to Article 39:

> *"Compared to the duties of the data protection officer in accordance with the BDSG, the GDPR waives individual operational tasks (employee training and prior checking) and primarily assigns the data protection officer a compliance task. [...] The data protection officer must check that there is sufficient awareness, and that proven employee training has taken place."*

The GVO commentary by Kühling/Buchner in marginal note 22 to Article 39 states:

> *"The data protection officer is not responsible for training staff, nor for the elaboration of data protection strategies, or for carrying out the data protection impact assessment. Overall, he does not have the authority to take action or to make decisions relating to his assigned role, and therefore does not have any responsibility for the success of the data processing. However, he must perform the tasks assigned to him properly, so as not to cause a liability risk for himself."*

The GVO commentary by Paal/Pauly in marginal note 6 to Article 39 states:

> *"The GDPR does not explicitly provide for the collaborative involvement of the data protection officer in the development of internal strategies"*

The clarification of responsibility is also of interest in this context. There are no clear statements on this (see Paal/Pauly in marginal note 11f to Article 39).

Does the data protection officer incur a special occupational risk from his supervisory function? Does he serve as a "**guarantor for supervision**" who can be held liable for data protection problems? This question is frequently raised in the technical literature. In its 09/2017 edition on page 411-414., "Zeitschrift für Datenschutz" does not see any significant changes in comparison to the Federal Data Protection Act.[46]

[46] The surveillance guarantor [Überwachungsgarant] is mentioned here, here and here, and is used in connection with Section 13 StGB and the term "false omission" [unechte Unterlassung].

Also see 09/2017 edition on page 411-414., "Zeitschrift für Datenschutz", where it is stated that there are no significant changes in comparison to the Federal Data Protection Act.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

12.0 Introduction

Forms

The description of the obligations in chapters 2-10 also covers the issue of how to correctly satisfy each specific obligation.

In many cases, extensive check lists or status forms are required. These documents were moved to chapter 12 for the following reasons:

- The move **saves space** in chapters 2-10. Thus, these chapters remain understandable.
- Some forms are relevant for **different obligations**. Therefore, it is useful to store these forms.
- Storage enables a **quick overview** of what forms are actually available in the PrivazyPlan®.

Each of the forms begins on a new page so you can print each form separately if required.

Each chapter starts with an introductory text. A heading in black can be found below. The form starts "officially" from here.

⚠ Please adapt the forms to your special operational needs. The examples we provide should only give a rough outline.

In this respect, the forms provided are really only a first approach for your operational needs. We explicitly request that you copy the contents of the form **in a clipboard** e.g. in a MS Word document. All modification to your business requirements can then be included here.

However, if you should be aware (as always) of possible updates to the PrivazyPlan® in order to transfer then into your personal form, if necessary.

The following are two tips for documents in MS Word:

- **Inserting the date your document was saved**
  The date your document was last saved should be inserted in the footer in the MS Word document. To do this in MS Word 2016, click "Insert | Quick Parts | Fields… | SaveDate".
- **Recommending read-only**
  You can protect the forms from accidental overwriting in MS Word 2016 by clicking on the link "More options..." in the Save dialog and then on the "Tools" and "General options" buttons and then activating "Recommend write protection".
  When the document is opened next, a dialog appears stating "The author would prefer it if you open this document with write protection." Very practical!

12.1 Basic checklists for PrivazyPlan®

Forms

The following checklist can help you to incorporate the GDPR and the PrivazyPlan® in the best way possible.

12.1.1 Fundamental reading on the topic

We recommend that you start the first 2-3 hours with extensive reading:[48]

⚠ Print out the following pages of the Appendix:

- the list of data processing examples starting on page 258
- the brief summary of all obligations starting on page 354
- the detailed table of contents starting on page 367
- the full table of obligations starting on page 370
- the index starting on page 378

... and keep those print-outs in easy reach.

☐ Read the **Foreword** from page 4. You will find lots of valuable information about the GDPR and the PrivazyPlan® here.

☐ **Bookmark** the following two websites:
www.privacy-regulation.eu
www.bdsg2018.de
so you can quickly access the original wording at any time.

☐ Read the **general information on GDPR** from page 348. This includes interesting details about the GDPR and the linguistic difficulties.

☐ Data protection as part of the GDPR is a **compliance issue** , as described in detail from page 295 .

☐ Read the **brief summary of all obligations** from page 354 (or on the print-out if you have followed the above recommendation). Once you have read this, then you will have gained a good impression of WHAT to do and HOW to do it.

☐ You will receive an **overall overview of the GDPR** in the brochure with the same title for €40. The entire GDPR is explained across 67 pages with 44 figures. It couldn't be any more compact.
You should check the added text of the regulation for translation errors (see page 305), or simply visit www.privacy-regulation.eu. Please note that you will be purchasing the *second* edition. The accompanying **eBook** available as a PDF in German and **English** is very useful! You must register with the publisher and then enter the "content code" from the inside book cover.
Further reading can be found on page 305.

12.1.2 Making HR decisions and starting work

The implementation of the PrivazyPlan® into the everyday operation of the business requires a large amount of effort across the company. It is initially a question of clarifying who is involved in this work.

In the chapter "A rough plan for implementing the GDPR" from page 16, the main actors are specified:

☐ Directors
☐ Data protection officer
☐ Information security officer
☐ Compliance officer.
☐ Data protection experts
☐ Data protection team
☐ Data protection project manager, if necessary
☐ EU representative, if necessary

[48] The following blue box is a cross-reference to the "original place" on page 10. From here, you can access the desired pages.

The controller is able to work as soon as these “Roles/Functions” have been assigned. The first steps are described in detail from page 16.
Does your business have a works council? Then you must decide who will ensure data protection.

12.1.3 Rough checklist for the first steps

a) Management’s first steps

Management needs to lay out a proper course of action before getting into the actual work:

☐ The **fundamental questions** raised in chapter 1.5 on page 14 should be clarified in the lead-up. This includes the important questions whether it is advisable to use the mini data protection management system proposed here in PrivazyPlan® (see chapter 1.10 on page 26)?

☐Has management read the short summary of the approx. 50 obligations as described on page 354 of chapter 14.1?

☐ Is the **“rough plan”** outlined in chapter 1.6.1 on page 16 proposed to be implemented? This rough plan deals with numerous responsibilities (Data protection officer, compliance specialist, IT security specialist, etc.).

☐ Will management issue an official **policy** and announce it to personnel? See chapter 12.2 on page 228.

☐ Who is supposed to read PrivazyPlan®? How can it be ensured that the relevant personnel are aware of the monthly changes?

☐ Before the departments start concrete work on the obligations, management should compile a “**rough plan**” (meaning the “plan” in the PDCA cycle). This ensures that the obligations are worked on in a uniform approach across the entire company. This would save time and hassle.
In concrete terms, this may mean that the “plan” content is completed in all relevant obligation spreadsheets in the mini data protection management system contained in PrivazyPlan.xls (see page 26).

After the above points have been clarified, you can start working on the approx. 50 obligations stipulated in the GDPR.

b) Designating a data protection officer, if necessary

PrivazyPlan® identifies 10 obligations associated with the designation and organisational integration of a data protection officer. All of this is explained in detail in chapter 8 starting on page 173.

☐ Should a data protection officer be designated on teh basis of a legal requirement (see obligation **[GVO_037]** on page 174)? Or should this be voluntary?

c) Identifying data processing operations / work on 40 obligations

Out of the approx. 50 obligations imposed by the GDPR, around 40 are based on the specific data processing operations conducted by the controller.

This is illustrated in the example of a **website contact form**: (a) The data processing must be documented in the record of processing, (b) different information notices have to be prepared, (c) the privacy rights of information, deletion, correction, etc. must be warranted.... and many more.

This means that the identification of data processing operations plays a major role. It “sets the goalposts” of the data protection “game”.

☐ **Identify** the data processing operations. PrivazyPlan® provides you with a fairly extensive list and concrete examples (see page 258) and the “structural analysis” approach (See page 261).

☐ Complete the work on the 40 obligations for each single data processing operation. The work can be based on either the processing **master record** (see page 263), or the MS Excel table **PrivazyPlan.xls** that is part of the “mini data protection management system” (see page 26).

d) Information management system (ISMS)

Article 32 requires the controller to plan the security of a data processing operation in a risk-based approach, to warrant security without interruptions and regularly assess security (see obligation **[GVO_032]** on page 124).

This can only be achieved by using an ISMS. The topic “ISMS” is covered in detail in chapter 13.4 on page 309.

☐ You decide **which** ISMS is suitable for your purposes.

☐ Start **implementing** the ISMS as soon as possible. The information security officer has to complete this task by 25 May 2018.

d) Miscellaneous

The following is a (possibly incomplete) list of the obligations that should be completed at some stage before 25 May 2018:

☐The "**xxx [GVO_005]**" starting on page 81 must be established.

Sorry, the hyperlinks in chapter 12.1 of this demo do not work.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

13.0 Introduction

Technical information

The following documents provide technical information that assists in forming a general understanding.

The sequence of chapters serves no specific purpose but resulted spontaneously from the topics that need to be covered by PrivazyPlan®.

13.1 Important (legal) changes

Technical information

European data protection is not a “finished system”. New laws, important court rulings or other comments must be expected at any time.

The list below can be taken as an opportunity to inform company employees; see VdS guideline 10010 (see page 291) in chapter 8 contained therein (“Knowledge”).

This chapter serves the continual documentation of important changes.

13.1.1 Third quarter of 2017

- 15.12.2017
  New in February: **VdS guideline 10010** (pronounced “ten zero ten”) has been enacted. The free download can be found here. 32 pages provide structured descriptions of how data protection management systems can be established within companies. The PrivazyPlan® features more than 20 references to the corresponding chapters. The VdS guideline is the perfect supplement to the PrivazyPlan®. The VdS also offers 2-day seminars. When it comes to the provability of compliance as part of obligation [GVO_005], VdS 10010 certainly makes a good case. Back to the foreword

- 01.11.2017
  The Article-29 Working Group has made the German translation available for three working papers (WP 242, WP 243 and WP 244). It is becoming increasingly difficult to maintain an overview of the numerous working papers. For this reason, all up-to-date versions have been summarised at http://www.privazyplan.eu/article29/. This document collection will be continuously updated in the future.

- 03.10.2017
  The Article-29-Group has some new working papers available for discussion on 3 October 2017 (the final versions are not expected before the end of 2017):
  - „WP 250“ for reporting data protection violations (Article 33, page 135)
  - „WP 251“ for automated decision (Article 22, page 76)
  - „WP 252“ for Cooperative Intelligent Transport Systems
  - „WP 253“ for fines and their criteria (Article 83, page 76)

- 01.09.2017
- The German Conference on Data Protection has published a number of short papers commenting on the GDPR: Certifications according to Article 42, notification obligations according to Article 13 and Article 14 and the right to be forgotten according to Article 17.
  These short papers should be considered by the company when implementing GDPR.

- 31.08.2017
  The “Data Protection Amendment Act 2018” has been pronounced in Austria. The opening clauses of the GDPR are used in 70 paragraphs on 31 pages. There is no special regulation concerning the data protection officer. See here as well.

- 31.07.2017
  The German Conference on Data Protection has published a number of short papers commenting on the GDPR: Record of processing, supervisory powers/sanctions, advertising, transmission into a third country, data protection impact assessment, right of access, lex loci solutionis and plan of measures.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

13.2 Compliance (rule-compliant data protection)

Technical information

The real value of PrivazyPlan® only becomes apparent once the legal context has been understood. The new European data protection law places high demands on companies, authorities and other parties involved.

13.2.1 What is compliance? Why is this issue important?

Some readers may have come across the issue of “compliance” in the context of the law on stock corporations, the combat against insider trading, prohibition on cartels, money laundering or corruption. The introduction of the EU General Data Protection Regulation (GDPR) means that the issue of compliance is now of relevance for all companies.

“Compliance” means a bundle of measures taken by a company for the purpose of ensuring its business operations are conducted in a lawful and faithful manner and to monitor the same. The objective is to prevent any conduct that may incur fines or penalties, claims for damages or entail serious financial or reputational damage.

It may not be a coincidence that Article 5 (1a) postulates precisely the following:

*“Personal data must be processed **lawfully** and in **good faith**”.*

Bull’s eye! There can be no doubt: Data protection is a compliance issue. [57]

PrivazyPlan® takes this into account in obligation **[GVO_005b]** (see page 81).

In the English version of the regulation, the words “compliance” and “comply” can be found at 79 locations.
The German translation uses the rather inconspicuous terms “*einhalten*”, “*erfüllen*” or “*im Einklang stehen*”. It is telling that there is no corresponding word in German.

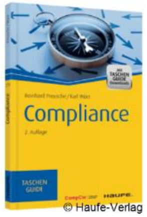
Many of the provisions of the GDPR leave no doubt that fines and claims for damages can be imposed (see page 333).

When compared to the times of the Federal Data Protection Act, the following becomes apparent: The times in which a company would implement data protection on the basis of gut feeling and pot luck are over; companies can no longer rely on German supervisory authorities and their practice of rarely imposing fines according to Section 43 BDSG (and if they did, the fines were very moderate). Gone are the times in which claims for damages according to Section 7 BDSG were only possible in cases where demonstrable material damage was incurred.

Seen this way, data protection compliance in the times of the GDPR is not a luxury but rather an important measure safeguarding a company’s survival.

Given the extremely diverse obligations with regard to transparency prescribed by the GDPR, a controller should not hold his breath that his unlawful or dishonest processing of data will remain undetected. He should rather expect the opposite to happen. The leverage of social networks on the internet (Facebook, etc.) entails the increasing risk that negative experiences of users or customers get around in these forums and result in serious **reputational damage**.

[57] The commentary by Kühling/Buchner in marginal note 15 to Article 5 assumes that the wording “in good faith” is intended to prevent a **concealed** instance of data processing.



The compact booklet "**Compliance**" published by Haufe-Verlag is highly recommended. It can be purchased for 7.95 € as hardcopy or 3.99 € as an eBook in PDF format. It's the perfect start to learn about the issue! It explains everything on only 128 pages.
Other interesting sources of information can be found here, here, here, and here.

(The DSB-MIT-SYSTEM offers a newsletter to raise staff awareness: NEWS_034).

The first compliance requirements prescribed by law in Germany were those for the prevention of insider trading stipulated in the Security Trading Act of 1994. A look beyond Germany shows: Other countries' lawmakers consider compliance to be indispensable. Spain introduced a criminal law for corporations in 2016, which makes the establishment of a compliance management system mandatory. Italy even has an explicit Compliance Act.

By now, banks and insurances have also become interested in the compliance management of their customers. A cyber insurance now requires a company to have an information security management system (ISMS) in place (see page 309).

The "compliance virus" appears to be spreading on a global scale. The introduction of the GDPR means that compliance has now found its way into data protection.

13.2.2 Who is liable for compliance violations ?

The question of determining liability starts with considering Section 93 of the Stock Corporations Act [AktG] or Section 43 of the Private Limited Companies Act [GmbHG] in the case of a German GmbH.

> *"The directors shall conduct the company's affairs with the due care of a prudent businessman. Directors who breach the duties incumbent upon them shall be severally and jointly liable to the company for any damage arising."* [source: Section 43 para. 1 and 2 GmbhG

The concrete liability of company owners (or the managing directors) is stipulated in Section 130 of the Administrative Offences Act [OWiG], They are obliged to take adequate supervisory measures to prevent a punishable infringement against their company's obligations.

> *"Whoever, as the owner of an operation or undertaking, intentionally or negligently omits to take the supervisory measures required to prevent **contraventions**, within the operation or undertaking, **of duties** incumbent on the owner and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as **would have been prevented, or made much more difficult, if there had been proper supervision.***
> *The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel. [...]*
> *The infringement against an obligation carries a regulatory fine not exceeding one million Euro [...]" [source: Section 130 para. 1 and 3 OwiG]*

Section 9 OwiG (also) imposes this responsibility to the instructed personnel. A ruling by the Federal Supreme Court concerning the Berlin Street Sweeping Company (5 StR 394/08 dated 17 July 2009) addresses the "guarantor's obligation" according to Section 13 para. 1 StGB (see chapter 1.5.3 of the TOM-Guide®):

> *"Whosoever fails to avert a result which is an element of a criminal provision shall only be liable under this law if he is responsible under law to ensure that the result does not occur, and if the omission is equivalent to the realisation of the statutory elements of the offence through a positive act."*

Section 30 OwiG also provides for fines of up to 10 million Euro to be imposed against the company as a legal entity.

Some companies appoint an explicit compliance representative (see here), who will in certain circumstances bear joint liability (see here).

The book "Compliance" (p. 25) recommended above suggests taking out a director's and officer's liability insurance for executives. Elaborate professional articles explaining the liability risks of a company's executives can be reviewed here and here.

New in February: The **German Supreme Court** has ruled that an effective compliance management system can protect against fines (09/05/2017 – 1 StR 265/16):

"Also of significance to calculating the fine is the extent to which secondary participants satisfy their obligation to prevent legal infringement from within the company sphere, and whether they have installed an efficient compliance management [system], which must be designed to prevent legal breaches".

Reviews of this ruling can be found here, here, here and here.[58]

Conclusion: A company's management bears a supervisory obligation to prevent punishable infringements against obligations, or to at least make an infringement significantly more difficult. This obligation can (at least partially) be delegated to carefully selected supervisory persons.

13.2.3 How can compliance be assured?

The permanent assurance of compliance is a complex endeavour. A comprehensive range of literature and software is available, in particular on the issue of combating money laundering and corruption. The overall context raises the question of a compliance management system (CMS).

© Beck-Verlag

Fortunately, a reference book dealing with the issue specifically from a data protection perspective became available in March 2017. The book "Data protection compliance pursuant to GDPR" by Sachs / Kranig / Gerschmann provides a very good insight over 226 pages for only € 44 (available as hard copy or PDF e-book).

All important aspects are covered in remarkable detail. The book is highly recommended for all companies that are serious about introducing a compliance management system.

The 226 pages are of course not enough to cover every single aspect of the issue in all detail. One of the book's shortcomings is that it fails to address the obligations of the data protection officer, which also have to be mapped by a CMS.

[58] See Datenschutz-PRAXIS 01/2018 pages 17-19

Further reading can be found in works like the reference book "Effective compliance management systems", available as eBook or hard copy for € 52. The reference book "Practical knowledge: Compliance" published by Haufe-Verlag could also be of interest and is available as hard copy for € 49.95 or as an eBook (PDF or EPUB) for € 44.99.

The introduction of the **DIN ISO 19600** in mid-March 2016 provided an international standard for CMS; this approach corresponds broadly with the auditing standard 980 published by the Institute of Public Auditors in Germany (IDW). A 52-page brochure on the DIN standard explains the backgrounds by examining 21 questions (€ 20 for book and PDF eBook).[59]

Conclusion: There is plenty of literature and know-how on the issue of "compliance". The development of a real compliance management system CMS) unfortunately requires a lot of time, money and persistence.

13.2.4 Compliance ensured by using PrivazyPlan®?

Starting in August 2017, PrivazyPlan® will be available to assist with the implementation of the GDPR. How can PrivazyPlan® assure data protection compliance?

The idea is as follows: If the controller first identifies and then performs all the obligations stipulated in the GDPR, all risks of fines and claims for damages would essentially be under control. The company is then compliant in terms of data processing (especially if compliance is continually monitored and optimised in the context of a PDCA cycle).

In this sense, PrivazyPlan® can indeed assist in preventing compliance violations.

The very broad accountability stipulated in Article 5 (2) means that the controller is required to document his strategies and measures. This is the prerequisite for a fine to be reduced by the supervisory authority according to Article 83 (2) (see page 333). The well-known principle "Write it down and keep your job" rings true once again. This aspect is also covered PrivazyPlan®.

[59] The basic principles are illustrated on page 36 of the brochure.

This alone does however not make for a compliance management system. PrivazyPlan® does not clarify how the controller is supposed to organise his company as a whole in a way that would ensure a compliance-aware "environment". This aspect is rather covered in the chapter above.

13.2.5 What has to be done?

There importance of data protection compliance appears to be undisputed. But what's the best way of tackling the issue?

1. **In which areas does the company want to improve its compliance?**
   In a first step, the issues to be tackled in the future should be determined. This could, for example, be the following areas:
   Occupational safety, fire protection, data protection, export and import controls, money laundering prevention, corruption prevention, product safety, quality management, contract management, unfair competition, environmental protection, white-collar crime and customs.

2. **How extensive should compliance management be?**
   The scope of areas to monitor (see above) assists in determining the complexity of the compliance management system. The more areas are to be covered, the more systematic the controller must approach the issue. This would be a good time to obtain expert knowledge and external expertise.

   The reference book "Data protection compliance pursuant to GDPR" mentioned above is highly recommended with regard to data protection.

3. **Focusing on the essential issues?** PrivazyPlan®.
   The company has no resources for a "real" compliance management systems with all the bells and whistles? In this case, the controller should at least tackle the essential obligations prescribed by the GDPR. This will afford a certain level of control over the immediate risks of incurring fines or claims for damages. This is precisely what PrivazyPlan® has been designed for.

4. **The starting point**
   Time is of the essence. The controller must establish (verifiable) data protection compliance by 25 May 2018. From the perspective of PrivazyPlan®, the procedure looks like this:

   (a) Extract concrete obligations from the GDPR. PrivazyPlan® has already completed this step.

   (b) Prioritise the obligations (courage to leave gaps?). PrivazyPlan® provides a ready-made concept for prioritising the obligations. See page 16.

   (c) Start with the more time-consuming obligations. PrivazyPlan® specifies the more time-consuming obligations.

   (d) The following applies to each individual obligation of the GDPR: Start with the planning step, then the preparation step followed by the implementation step. PrivazyPlan® offers specific PDCA checklists for this purpose. See chapter 12 starting on page 223.

   (e) Preparing and applying checklists and status sheets. *PrivazyPlan®* offers specific PDCA checklists for this purpose. See chapter 12.

   (f) Appointment of a data protection officer for monitoring compliance The specific GDPR-related responsibilities of the data protection officer are described in chapter 11 of PrivazyPlan®. The performance of obligations can be monitored (in a risk-based approach) by using the software DSB-Reporter®.

   Concurrently to these activities, the responsible entity should evaluate the introduction of a data protection ticket system (see page 337). The same goes for a central document management system (see page 337).

There is much to be done. Let's get into it!

13.2.6 Ultra-short checklist for data protection compliance

How can you gauge, at least roughly, whether a company is compliant in terms of its data protection? Given the enormous complexity of the issue, a checklist can only ever touch on the most essential questions. As data protection compliance requires a continual effort for the purposes of the PDCA cycle, the following checklist has been structured on the basis of this pattern:

a) Planning a strategy ("plan")

The following questions pertain to planning. This is where the fundamental decisions will be made and the course is charted:

1.) Did the company's management make a clear and "official" commitment to establishing data protection compliance? Do the plans envisage a "real data protection compliance management" or merely the performance of the most important obligations? Is there a corresponding corporate policy?

2.) Are there readily apparent organisational structures that show the company has in fact designated the responsible and competent staff members? Has a compliance officer been appointed? Is there a team of experts from all departments? Have the rights and obligations of these employees been set out in a signed written document?

3.) How are these employees supposed to acquire the necessary specialist knowledge? Does the company make adequate technical literature available, or does it conduct training events? Does the data protection officer make necessary know-how available (i.e. TOM-Guide®)?

4.) Is there a data protection ticket system for the swift, reliable and transparent processing of inquiries received from data subjects?

5.) Is there a document management system for the central archiving of all necessary resources, such as copies of the law, agreements, consent declaration contents, checklists (blank and completed)?

6.) The European data protection is not a "finished system". What is the reaction to changes in the law? Who is responsible for researching all relevant changes and making them available to the company?
This concerns changes to (a) the GDPR and (b) national laws of all EU member states that are supplied with goods or services by the company and (c) the position papers of the Article-29-data protection group and (d) the position papers of the German supervisory authorities and (2) court rulings.... among many others.

7.) Has a data protection officer (with the necessary expertise and reliability) been appointed? If this is not required (and is not proposed on a voluntary basis): Who is the company's data protection expert?

8.) What are the responsibilities assumed by the data protection officer? Does the controller have a clear picture of what the data protection officer does? How will he perform the obligation of instructing, advising and supervising? What does the data protection officer **not** do?

b) Implementation ("do")

The following explains the actual implementation step. Data protection is now making itself noticed in the staff's daily work routines:

1.) Have the employees been informed about the GDPR and other regulations? Have training events been conducted? Are newsletters planned?

2.) Does the controller have a precise overview of all (at least 50) specific legal obligations prescribed by the GDPR and other regulation? How is the necessary data protection know-how imparted to the employees for them to understand the respective obligation? Compliance is out of reach without this detailed knowledge. Examples of particularly "critical" obligations are listed below:
- Information management system (ISMS),
- Record of processing,
- Providing for copies of data and data export

3.) Are the obligations prioritised? Are the more time-consuming obligations performed first? Are there specific target deadlines for performing these obligations? Is there some kind of project management to monitor the timely performance of obligations? The cut-off date is 25 May 2018.

4.) How will obligations identified as relevant be performed? Does the company employ a systematic approach? Who decides on how the respective obligation is performed? Are checklists and a structure for the purposes of the PDCA cycle available?

5.) Is the record of processing administered in accordance with Article 30? Does the person in charge possess the necessary expertise and overview necessary for the correct documentation of it all? Will the result be shared

with the respective departments in a reasonable format, enabling the departments to do their work properly?

PrivazyPlan® provides approx. 50 specific obligations derived from the GDPR and other regulation (StGB, TMG, TKG, UWG, etc.). Each obligation has its own acronym (i.e. "GVO_015"); this makes it very easy to process them systematically. Explanations and processing instructions for each individual obligation can be found in chapters 210. Chapter 12 contains checklists and status sheets.

c) Monitoring ("check")

Consistent data protection compliance requires continual monitoring for the purposes of the PDCA cycle. This can be done in different ways:

1.) How does the company's management perform its supervisory obligation according to Section 93 AktG or Section 43 GmbHG and Section 130 OwiG? Is this done "passively" in the form of quarterly reports, as well as "actively" in the form of semi-annual meetings?

2.) Is there an internal monitoring system where the compliance manager (or other employees of the company) monitor whether the respective competent colleagues are performing the obligations assigned to them? This approach ensures a relatively close monitoring of whether, for example, the "data export manager" really assures the data of a data subject can actually be delivered on request. Does regular reporting take place?

3.) How does the data protection officer perform their supervisory obligation according to Article 39 (1b)? Does he systematically monitor the controller's performance of all (approx. 50) obligations? Does he also systematically monitor the controller's overarching strategies? Does regular reporting take place?
See obligation [GVO_003] on page 219.)

4.) Are there plans to obtain certifications in the meaning of Article 42?

d) Optimisation ("act")

What is the reaction if compliance is in need of optimisation?

1.) When a director assesses a need for optimisation: Does he inform the other directors (if any)? Does he have a budget allowing him to purchase software or know-how or to hire a new employee? If he modifies the company's organisational structure: Is this being documented for the purpose of demonstrating to a supervisory authority that data protection is "alive" in the company?

2.) How do internal employees submit their own suggestions for improvement within the context of the internal monitoring system? Is this initially discussed with the data protection officer? Is this followed by informing the head of the department (and, if necessary, the company's management)?

3.) How does the data protection officer report his suggestions for optimisation? The directors will in this regard start with defining the requirements pertaining to the severity, urgency and the persons or departments to be informed. This enables the data protection officer to provide the desired feedback on the basis of objective criteria.

In May 2017, the Bavarian data protection supervisory authority prepared a "questionnaire" for the purpose of ascertaining compliance with the GDPR; the companies now know what kind of questions they will be asked.

13.2.7 Compliance software

The software market offers different software solutions for conceptualising compliance and making it part of the corporate culture. Two exemplary products are described in the following:

a) viflow

Hanover-based ViCon GmbH offers a range of products for handling matters concerning compliance.

- "viflow" is based on MS Visio and provides a graphical illustration of the compliant handling of personal data. The illustrations are generated using a Microsoft Windows computer and are then available for general use in the form of HTML files. A license covers 5 users and is priced from € 690 (once-off purchase price).

- viflow is complemented by "viflow easy plan", which converts the obligations into tasks. A license covers 3 users and is priced from € 990 (once-off purchase price).
- "viflow DMS" allows for the generated text-based documents to be filed in a document management system for easy retrieval. A license covers 5 users and is priced from € 1,290 (once-off purchase price).

b) The GEORG compliance management system

The company Martin Manz GmbH from Grosswallstadt offers the "GEORG Compliance Manager". This software lets you set up comprehensive compliance management systems. It is designed to cover the area of "occupational safety" and offers hundreds of relevant obligations that can be performed and documented by the company. [Unfortunately, no prices are available yet...]

c) DocSetMinder®

The product DocSetMinder® is offered by GRC Partner GmbH based in Kiel. It is based on a relational database (MS SQLServer) and can be operated with Microsoft Windows clients. The company can be documented on the basis of customisable templates (with fields like location, employees, etc.). Different compliance modules can be added on the basis of the templates. It is clearly structured and intuitive to operate. It also shows the implementation status in the context of PDCA cycles and allows for the systematic documentation of, for example, data protection violations. The approx. 50 obligations set out in PrivazyPlan® are presumably easy to implement and work on.

The base module (for 5 users) costs € 6,500 once-off and approx. € 1,200 per year for maintenance and updates. The add-on modules (reporting, appointments/tasks, import/export, IT landscape, BSI base-level protection, ISO-27001, ISIS-12, occupational safety, ...) each cost between € 2,000 and 4,000. A data protection module developed in cooperation with the ULG is also available.

d) Use of Customer Relation Management Software (CRM) for non-intended purposes

It is likely that every CRM has all the features that you need for a compliance management system. There are open-source systems such as 1CRM which are available free-of-charge. Installation onto a server with PHP and mySQL is easy to perform.

How can the features of a CRM be used for the non-intended purposes of data protection compliance?

- Your own company is stored in the "Customer" forms (and perhaps other companies in the corporate group).
- The "Contacts" are not (potential) customer contacts but rather the company's own employees. This is where the most important managers and other key individuals can be stored. Thus, they would be available for a variety of purposes (e.g. allocating responsibilities as well as email newsletter addressees).
- The email campaigns would not be used to acquire customers but rather raise awareness among the company's own employees.
- The email client can be used to jointly edit data protection-relevant emails (e.g. for datenschutzverletzung@unternehmen.de).
- The "service cases" are used to document and process issues from data subjects (request for information, revocation etc.).
- The file versioning can be used to save consent declarations and information texts to act as permanent records.
- The data protection team would use task management to jointly complete tasks.
- The team calendar can be used to coordinate the data protection team. This allows complete training events to be planned and executed.
- The project planning features can be used by the data protection project manager to plan for the transition to GDPR and realise the scheduled goals.
- The ticket system is used where there is noticeable need for improvement in monitoring obligations.
- Could the record of processing itself be stored in a CRM? The existing data structures would have to be under a large amount of strain already. The user-defined data fields could be used, for example, to create the corresponding structures in a discussion thread in order to document the purpose and deletion deadlines of a data processing operation. [But perhaps there is a programmer who is programming a corresponding add-on...]

Even this short list of possible applications shows that CRM is suitable for use in compliance management. It just takes some imagination.

13.2.8 Conclusion on the issue of "compliance"

Let's summarise the issue of "compliance":

❶ What are the compliance-related changes that will be introduced on 25 May 2018?

- **Obligation to produce evidence** (It is no longer sufficient to merely be data protection-compliant. Article 5 (2) stipulates that companies must be able to produce evidence supporting compliance at any time. Technical literature commonly uses the term "obligation to produce evidence" interchangeably with "compliance".)
- **Systematic security** (Article 32 (1d)requires the technical and organisational measures to be subjected to a "regular review, assessment and evaluation". This necessitates a PDCA cycle. This is the essence of compliance.)
- **Developing strategies** (According to Recital 78, they must "determine internal strategies" for the purpose of evidencing compliance with the regulation. This necessarily leads to a PDCA cycle. The use of data protection guidelines is also helpful; see VdS guideline 10010 (see page 291) in chapter 6 contained therein "Guidelines".)
- **Controlling risks** (The data protection impact assessment postulated in Article 35 and other aspects presuppose a conscious approach to risks. In certain circumstances, very detailed considerations may be required.)
- **The strategies are supervised by the data protection officer** (Pursuant to Article 39 (1b) and other provisions, the data protection officer is also responsible for supervising the strategies employed by the controller. A full list of the data protection officer's obligations can be found starting on page 215.)
- **Performance of obligations** (Due to the above aspects, the GDPR must be broken down into its individual obligations. PrivazyPlan® does exactly that. A brief characterisation of all approx. 50 obligations can be found starting on page 354.)

Conclusion: Before 25 May 2018, the Federal Data Protection Act was exclusively concerned with the result ("the BDSG must be observed").
The GDPR however now also regulates the way towards that result (documentation, risk analysis, strategies, regular assessment via PDCA, obligation to produce evidence).

❷ What makes compliance worthwhile?

- **Preventing fines** (amounting to up to 4% of a group's annual revenues)
- **Preventing claims for damages** (now also for non-material damages)
- **Preventing audits by the supervisory authority** (because this wastes several days of otherwise productive time; also because external resources, such as a data protection officer, also have to be remunerated for their efforts).
- **Preventing bad press** (this is an important point in the times of Facebook and the like, as these media may ruin a painstakingly created corporate image within a matter of hours)
- **What makes your service indispensable?** (If your company generates revenues by processing personal data on behalf of other companies, then you will have to tick the box for data protection. Without verifiable data protection, your times as a market player may soon be over. It shouldn't come as a surprise when your orders flatline and existing contract are terminated or not renewed.)
- **Preventing business risks** (It will not take long for your auditor to discover the issue of data protection with its horrendous fines and potential claims for damages. He will ask you to demonstrate that you are in control of these risks.

  You will face the same situation if you ever want to sell your company: It is virtually guaranteed that sub-standard data protection will result in mark-downs on the purchase price.

- **Out of conviction** (yes, that happens. Some company owners take the stance "I demand may own data is afforded effective protection. How could I refuse my own employees and customers the same benefit?" Respect.)

❸ When will you kick-off?

- **Waiting for crisis to hit** (You hope things won't be as bad as you heard they might be. You hope nobody will notice the fact that your company does not comply with the GDPR. You believe that you can still perform the approx. 50 obligations after being caught. That's a risky and potentially expensive decision.)

- **Waiting for "*the* solution"** (While you do appreciate the relevance, you'd rather wait for a service provider with a "magic wand" to come along. You don't need to wait any longer as you'll be hard pressed to find a better plan than PrivazyPlan®. Get started now!?

- **Here and now !** (Go on the offensive. Use PrivazyPlan® and secure a head-start. The earlier you get started, the less pressure and the more time you and your staff will have.... prevent burn-outs and "mental resignations".)

❹ What has to be done?

- **Make a commitment** (The company's management makes a written commitment to data protection as a company goal. This is imperative for setting the company on course towards compliance.)

- **Develop an organisation** (Which staff member will become your "compliance" officer? This person will take the reins and dedicate his efforts to achieving data protection compliance. Appoint one staff member in each department as a point of contact. Create a team!)

- **Appoint a data protection officer** (Appoint a data protection manager according to Article 39, who will instruct, advise and supervise in relation to your obligations. If that person does not have a ready-to-go concept, invite him to learn about PrivazyPlan®.)

- **Acquire specialist knowledge** (Use PrivazyPlan® to bring your expertise up to speed. Start on page 354 of chapter 14.1, this is where you will find the shortest possible explanation of the approx. 50 obligations. Utilise the technical literature and information sources listed on page 305.)

- **Identify and prioritise your obligations** (A brief characterisation of all approx. 50 obligations can be reviewed starting on page 354.) Which obligations are tedious? Which ones have to be done by 25 May 2018? Which ones attract the highest fines? What lapses are virtually guaranteed to be detected? The data protection team determines the priorities and communicates them to the departments.)

- **Work through the obligations** (Assign the responsibilities within the departments: Which staff members are assigned to which specific obligations? PrivazyPlan® covers the individual obligations one-by-one; distributing them across a number of staff members is unproblematic. Set time limits and monitor them.)

❺ Can't the data protection officer do it all?

No, that would **not be permissible** for the following reasons:

- **Conflict of interests** (The responsibilities of the data protection officer are clearly set out in Article 39. Thy do not include the development of a data protection compliance system. On the contrary: His "supervisor" role actually prohibits the data protection officer from creating the contents he is supposed to supervise.
In a crisis, the supervisory authority would question the efficacy of his supervisory role. One of the most important pillars of data protection would be jeopardised.)

- **Independence and autonomy** (Recital 97 requires the data protection officer to be "completely independent" in the performance of his obligations and responsibilities. Article 38 (3) stipulates that no instructions may be issued to the data protection officer.
What would happen if the data protection officer were to design the compli-

ance measures for the company without direction and entirely independently? He would dictate a compliance management system to the company at his discretion; any technical influence by the company would be impossible. Is that desired?

It would in any case also not be practicable:

- No detailed knowledge about processes (The data protection measures must be interwoven into the existing processes (i.e. hiring of new staff, customer service, cold calling). But you are the only one who knows the exact way to do it and what it takes. Are you going to request your data protection officer to familiarise himself with all your business processes so he can plan the matching data protection measures for you? That would require him to have as much knowledge as all the other staff combined. Which would probably be asking for too much.)

- Limited operational involvement (The data protection officer can't be everywhere at once. But permanent vigilance is imperative! Who will raise the issue of data protection when new product ideas are floated? Who will recognise a problem when it occurs suddenly? Only staff members at the scene of the event can do that. But how can a REAL awareness be instilled in your staff members? Surely not by conducting training sessions and sending out newsletters. No, your staff members have to UNDERSTAND data protection and eventually make it part of their nature. This is why it's not helpful to burden the data protection officer with a knowing everything and doing all the work by himself.)

- Data protection is a team effort (Many data protection activities can only be performed reliably and timely if the company acts as a "team". Problems are destined to occur if each individual department just digs themselves in and works with "tunnel vision". But how are teams supposed to form if everyone follows the same philosophy: "The data protection officer will surely fix it"?

Conclusion: There is no way around it: Your own staff has to develop the plan-do-check-act cycles and fill them with substance. The data protection officer is (more than) busy enough with instructing, advising and supervision. See chapter 11 starting on page 215.

13.3 Technical literature and information sources

Technical information

Implementation of the GDPR is first and foremost the responsibility of a company's personnel. The use of technical literature is indispensable for acquiring the operational know-how. Where can you find the necessary know-how?

13.3.1 Online access to the regulation

Where can I quickly and easily access the GDPR and the amended BDSG?

➔ You can find the online resources in the introduction on page 10.

It is suggested that the staff members responsible for data protection bookmark the above websites in the favourites bar of their web browser for quick access to the regulation at any time.

a) Errors in the wording of the GDPR

We currently know of the following 10 material errors contained in the German version of the GDPR (also see here):

- Article 14 (1) should correctly start with "were" instead of "will be"
- Article 15 (4) should correctly refer to paragraph 3 rather than 1b
- Article 20 (4) should correctly refer to paragraph 1 rather than 2
- Article 28 (7) should correctly refer to Article 93 (2) rather than 87 (2)
- Article 30 (5) has been completely rewritten and now has an entirely different meaning
- Article 33 (1) should correctly refer to Article 55 rather than 51
- Article 37 (3) should correctly use the term "appoint" rather than "nominate"
- Article 62 (2) should correctly refer to paragraph 5 rather than 4
- Article 83 (1) should correctly refer to paragraph 4 and not only to paragraph 5 and 6
- Article 83 (2) should correctly refer to Letter j rather than i

Please make sure you take these errors into account when you access the original EU regulation or when you are reviewing the regulation on other websites.

13.3.2 Commentaries

The following works provide a solid entry point as well as comments on each individual section of the regulation.

At least one copy of the commentaries should be made available to the staff members responsible for data protection. Don't let the massive volume of the books deter you! The commentaries are very structured, which makes it easy to find the comments you are looking for in less than one minutes. The GDPR is incomprehensible and impossible to apply without using any commentaries.

- „**Datenschutzrecht**", Bergmann/Möhrle/Herb
  approx. 3,600 pages, € 96 (one year subscription)
  The September 2016 supplemental content includes commentaries on Articles 1, 30 and 32.
  It appears that each new supplemental content will cover new Articles.
- „**DSGVO / BDSG**", Eßer/Kramer/von Lewinski
  approx. 2,000 pages, € 149 (around September 2017)
- „**BDSG / DSGVO**", Plath
  approx. 1,700 pages, € 139
- "**Europäische Datenschutzgrundverordnung**", Sydow, approx. 1,500 pages, € 128
- „**Datenschutz-Grundverordnung: DS-GVO**", Ehrmann/Selmayr
  approx. 1,350 pages, 138 €
- „**Datenschutz-Grundverordnung: DS-GVO**", Kühling/Buchner
  approx. 1,200 pages, 159 €.
  A valuable source, which unfortunately occasionally makes reference to outdated content and interprets that outdated content.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

13.4 Information security management systems (ISMS)

Technical information

How can the permanent security of information be assured?

Technical and organisational measures must be implemented to assure the permanent security of data processing according to Article 32 (1). The risk entailed by the respective data processing operation must be adequately taken into account. This can only be warranted by implementing an „information management system" (ISMS).

➔ See obligation [GVO_032] on page 124.

➔ The selection of an information security management system is explained in detail in chapter 12.14, page 257.

The following sub chapters are intended to provide an overview: What types of ISMS are available on the market? How difficult is their implementation? What do they cost?

13.4.1 Listing technical and organisational measures

The list of technical and organisational measures is reproduced below for the sake of completeness. It goes without saying that the lists by themselves are not an ISMS. Conclusive evidence for an information security strategy is nowhere to be found. Nevertheless, a list of measures is better than nothing at all.

- **Ultra-short checklist**
  Some controllers will try to reduce the necessary effort to the absolute minimum. A checklist for this purpose is available in chapter 12.15.2 on page 272.

- **Short checklist of the VdS**
  Chapters 4 ("Organisation of information security") to 18 ("security incidents") of the catalogue of requirements to the VdS-3473 (see below) contains 15 interesting headlines that assist in your own deliberations concerning the organisation of IT security. This is a very good foundation for a comprehensive IT safety concept.

13.4.2 Minimum solutions on the basis of questionnaires

The following questionnaires are not an ISMS, but at the minimum they serve the purpose of enabling a company to evidence it has systematically considered the issued relating to IT security. Smaller service providers with 1-5 employees can be expected to operate at this level. When the question is about using these kind of service providers as processors in the meaning of Article 28 GDPR the least you should do is request such evidence to be produced (see obligation [GVO_028] on page 157).

- **ISA* - Information Security Analysis (not yet certifiable)**
  This questionnaire assesses the 50 most important aspects of IT security (order a copy free of charge by emailing felix.struve@it-sec-cluster.de). Experienced advisers stand ready to assist with completing the questionnaire. A certification is planned, but not yet available as of June 2016.[60]
  We were given the information that the first two certifications are planned for 2017. They will be conducted by DQS GmbH (costs are not expected to exceed € 2,000.)
  (Service provider PSW considers this a suitable approach for companies up to 50 employees. An evaluation of the completed questionnaire is available

[60] The 91-page guide "Leitfaden Informationssicherheit" is interesting and explains many of the basic aspects. Checklists that are similar to the ISA+ questions can be found in chapter 10.1 of the Annex.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

13.5 Data-Transfer – a fact sheet

Technical information

What legal options are available to a controller who intends to "share" the personal data held by him with other companies?

The GDPR does not provide precise information on how the **data transfer** to recipients outside of the own company should be handled. Unfortunately, the technical literature has so far failed address this issue in sufficient detail.

ATTENTION: The "Fact sheet on the disclosure of data" is only an attempt at untangling the confusing terminology used in the GDPR. The circumstances pertaining to **(a)** the disclose of data to recipients and **(b)** the common access together with other controllers and **(c)** the publication of data on the internet and in registers is EXTREMELY complex. The GDPR makes no effort to deliver an integrated concept, let alone definitions. This is further aggravated by systematic problems in the German translations. The above means that the fact sheet **should not be relied upon**.

The following chapters are structured identically: We provide the definitions, point to the passages, state the formal prerequisites, show the legal permissibility, explain the question of liability and state the corresponding obligation in PrivazyPlan®. We have intentionally kept it as brief and concise as possible so the big picture doesn't get lost in too much detail information.

13.5.1 Disclosure to "recipients"

A recipient for the purposes of Article 4 no. 9 is *"an individual or legal entity, authority, institution or other entity to whom personal data is **disclosed**, irrespective of whether such person is a third party or not".*

This means a purposeful disclosure of personal data to a specific recipient outside of the own company. The most important passages on this issue can be found in the [redacted]. There are three different scenarios:

a) Transmission to third parties within the EU or EEA

Unfortunately, the GDPR does not explicitly define or describe this scenario of "transmitting". It appears that a transmission according to Article 4 No. 2 is a normal processing operation: *"Processing is [...] the disclosure by way of transmission".* That's all.

The recipients are "third parties" according to Article 4 No. 10: *"an individual or legal entity, authority, institution or other entity [...]".* This basically means anyone outside the own company. (Exception: Authorities with an investigation mandate pursuant to Recital 31.)

The similarity to Section 3 para. 4 No. 3 BDSG (applicable in Germany until 25 May 2018) is obvious.

"Transmission" is a routine operation in companies. This, for example, includes the statutory transmission of employee data to health insurance funds.

The most important passages on this issue can be found in the dossier "Transmission". The original text in English uses the term "transmit" and "transmission". This was consistently translated as "Übermittlung" in the German translation (regrettably identically to the English term "transfer" in relation to the transmission to third countries or international organisations, see below).

There is no **formal requirement** to enter into an agreement or contract. Data is transmitted in an entirely informal way.(The GDPR does not provide for anything

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

13.6 Applying a risk matrix

Technical information

Quantifying risks is a difficult task. The term “risk matrix” is frequently found in technical literature. What is a risk matrix?

The term “risk” plays a significant tole in the GDPR (see chapter 6.1 starting on page 142). An objective assessment of a risk is a difficult task as it entails working with a large number of uncertain terms.

The risk assessment plays an important role

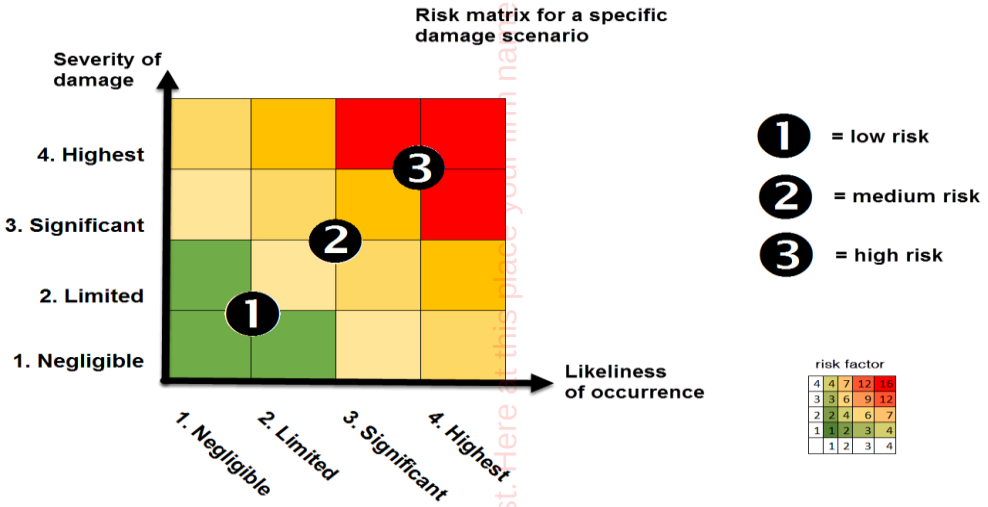
- in Article 33 (1) of the GDPR in terms of reporting a data protection violation to the supervisory authorities (if the risk is assessed as medium or high). The same goes for Article 34 (1) of the GDPR in terms of reporting a data protection violation to the data subjects (if the risk is assessed as high)
  See obligation **[GVO_033a]** on page 135.
- and for Article 35 (1) of the GDPR with regard to the data processing impact assessment, provided the data processing is expected to entail a high risk.

  See obligation **[GVO_035]** on page 142.
- and for the data protection officer, whom Article 39 (2) requires to perform his responsibilities in a risk-oriented manner.
- and in IT security for the purposes of assessing the risk of IT systems. All IT security management systems use risk assessments to estimate the extent of security measures. See page 309.

Many experts propose the use of a risk matrix, which classifies a specific damage scenario according to its “likeliness of occurrence” and “severity of damage”.

Each of the above four examples is different in terms of (a) the type of risk, (b) the risk scenarios, (c) the likelihood criteria, (d) the type of damage and (e) the possible counter-measures. For this reason, the application of a risk matrix can only be described in general terms.

The following illustration shows a typical risk matrix:



Such a risk matrix is of course only expedient if the underlying components are characterised plausibly and extensively. Most authors unfortunately fail to address this problem (possibly because that would quickly render the apparent simplicity of the risk matrix much more complex).

Seen this way, the “real know-how” is not in knowing the simple table above, but in how to correctly apply it. We will explain this in the following.

13.6.1 The “fundamental” application of a risk matrix

Similar to a cooking recipe, a list of ingredients and preparation instructions are needed for performing a risk assessment.

PRIVAZYPLAN®

GETS YOUR DATA PROTECTION ON COURSE.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

A brief summary of the obligations can be found on page 354; there is also a summary table on page 370.

The PrivazyPlan® basic checklists for a quick start into the topic can be found on page 225.

The Annex contains various approaches that will assist you in keeping an overview of the obligations.

In the end, none of the texts in the Annex contains any new information, but offers you a condensed overview.

These pages have intentionally been designed in portrait format with a wider margin on the left hand side for convenient printing and filing.

14.1 Brief summary of all obligations

Annex

Chapters 2 to 10 (on pages 29 to 204) offer a detailed description of the obligations of the controller with associated instructions. A click on the respective paragraph will lead you directly to the chapters covering the obligations.

14.1.1 Obligations based on privacy rights

The “rights of data subjects” are explained in chapter III, Articles 12-23 of the GDPR. Each Article prescribes one or a number of obligations:

Providing comprehensive information when collecting data [GVO_013]

According to Article 13 (1) and Article 13 (2) the company must inform the data subject in extensive detail right from the point when data is collected. The aim of that is to ensure fairness and transparency of data processing. We could look on that information as a sort of “enclosed leaflet” as provided with medication.

➔ Obligation [GVO_013] is explained on page 30.

Very briefly, it is about the following: ● Obtain the record of processing to identify all data processing operations concerned. ● Prepare the required information notice (as far as it has not already been prepared together with a “transparency” notice, see page 267). ● Make the notices available to the data subjects in a suitable format (i.e. on the website). ● All new/modified data processing operations must be prepared and published as soon as possible.

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

14.2 Detailed table of contents

Annex

Due to limited space, only an abridged table of contents is printed on page 2.
The following comprehensive table of contents will provide a better overview.
It may find it helpful to print this table of contents (see page 10).

14.3 Table of obligations

Annex

We recommend printing this page for a better overview (additional advice for a good overview can be found on page 10).

Obligations based on privacy rights

All “typical” privacy rights are explained in chapter 2.

Obligations concerning documentation and evidence

Chapter 3 explains the general “documentation requirements”:

Obligations concerning legality and consent

Chapter 4 explains the issue of legality (incl. the numerous aspects concerning consent):

Obligations concerning security and data protection violations

Chapter 5 explains the issues of information security and data protection violations:

5.1	xxx [GVO_032]	Article 32 (1)	124
5.2	xxx [GVO_032a]	Article 32 (4)	128
5.3	xxx [GVO_033]	Article 33 (5)	132
5.4	xxx [GVO_033a]	Article 33 (1)	135
5.4	xxx [GVO_034]	Article 34 (1)	138

Obligations concerning the impact assessment and consultation

Chapter 6 covers the data processing impact assessment and involvement of the supervisory authority, where necessary:

6.1	xxx [GVO_035]	Article 35.	142
6.2	xxx [GVO_036]	Article 36.	146

Obligations with regard to other controllers

Chapter 7 is dedicated to all kinds of “outsourcing”.

7.1	xxx [GVO_026]	Article 26.	149
7.2	xxx [GVO_027]	Article 27.	154
7.3	xxx [GVO_028]	Article 28.	157
7.4	xxx [GVO_028a]	Article 28 (3a).	161
7.5	xxx [GVO_028b]	Article 28 (3)	167
7.6	xxx [GVO_044]	Article 44.	169

Obligations concerning the data protection officer, etc.

Chapter 8 describes the operational involvement of the data protection officer (DPO) and explains his responsibilities:

8.1	xxx [GVO_037]	Article 37 (1)	174
8.2	xxx [GVO_037a]	Article 37 (7)	181
8.3	xxx [GVO_038]	Article 38 (1)	181
8.4	xxx [GVO_038a]	Article 38 (2)	184
8.5	xxx [GVO_038b]	Article 38 (4)	186
8.6	xxx [GVO_039]	Article 39 (1a).	188
8.7	xxx [GVO_039a]	Article 39 (1b).	190
8.8	xxx [GVO_039b]	Article 39 (1e).	193

Obligations stemming from other data protection rules

Chapter 9 covers the data protection-relevant provisions from other laws. The examples given may bear relevance for companies in Germany:

9.4.3	a) Obligations of a website service provider [TMG_013]	Section 13 TMG	198
9.4.3	b) Professional obligation to confidentiality [STGB_203]	Section 203 StGB	199
9.4.3	c) Unacceptable harassment for advertising purposes [UWG_007]	Section 7 UWG	199

Obligations stemming from the amended German Data Protection Act

Chapter 10 covers the data protection-relevant provisions used by the German legislator on the basis of an opening clause. The examples given may bear relevance for companies in Germany:

10.1	xxx [BDSG_004]	Section 4 para. 2	202
10.2	xxx [BDSG_004a]	Section 4 para. 4	204
10.3	xxx [BDSG_022]	Section 22 para. 2	206
10.4	xxx [BDSG_027]	Section 27 para. 3	208
10.5	xxx [BDSG_030]	Section 30 para. 1	209
10.6	xxx [BDSG_030a]	Section 30 para. 2	210
10.7	xxx [BDSG_035]	Section 35 para. 2	211

14.4 Uncertain circumstances (red bombs)

Annex

There are many unanswered questions concerning EU-wide data protection from 25 May 2018 onwards. Some of them are highlighted in PrivazyPlan® by little red bombs ( ) (see page 8).

A condensed summary of all bombs is provided in the following. Please click on the respective text for additional information to assist with a better contextual understanding.

14.4.1 Obligations based on privacy rights (chapter 2)

The identification of obligations is associated with a **degree of uncertainty**. Numerous provisions of the GDPR are not clear on whether a practical obligation might be involved in the case concerned. In at least 21 places in the Regulation, for example, a requirement for “evidence” is stated or at least implied. In more than one instance, the reader could easily interpret this as an obligation to provide evidence. (Page 11)

[redacted] (Page 38)

[redacted] (Page 66)

New in January: What constitutes “making data available”, which leads to a right to data portability? Is it only relevant to data consciously provided by the data subject? It is undisputed that data typed by the data subject themselves is affected. But what about logfiles generated unknowingly in the background? What about the video data created when a person is located within the visual range of a video camera? What about geo data from a fitness watch transmitted to the provider? (Page 68)

... this is an excerpt.

If you want to get a license of PrivazyPlan®,
so please visit us at
www.privazyplan.eu/en

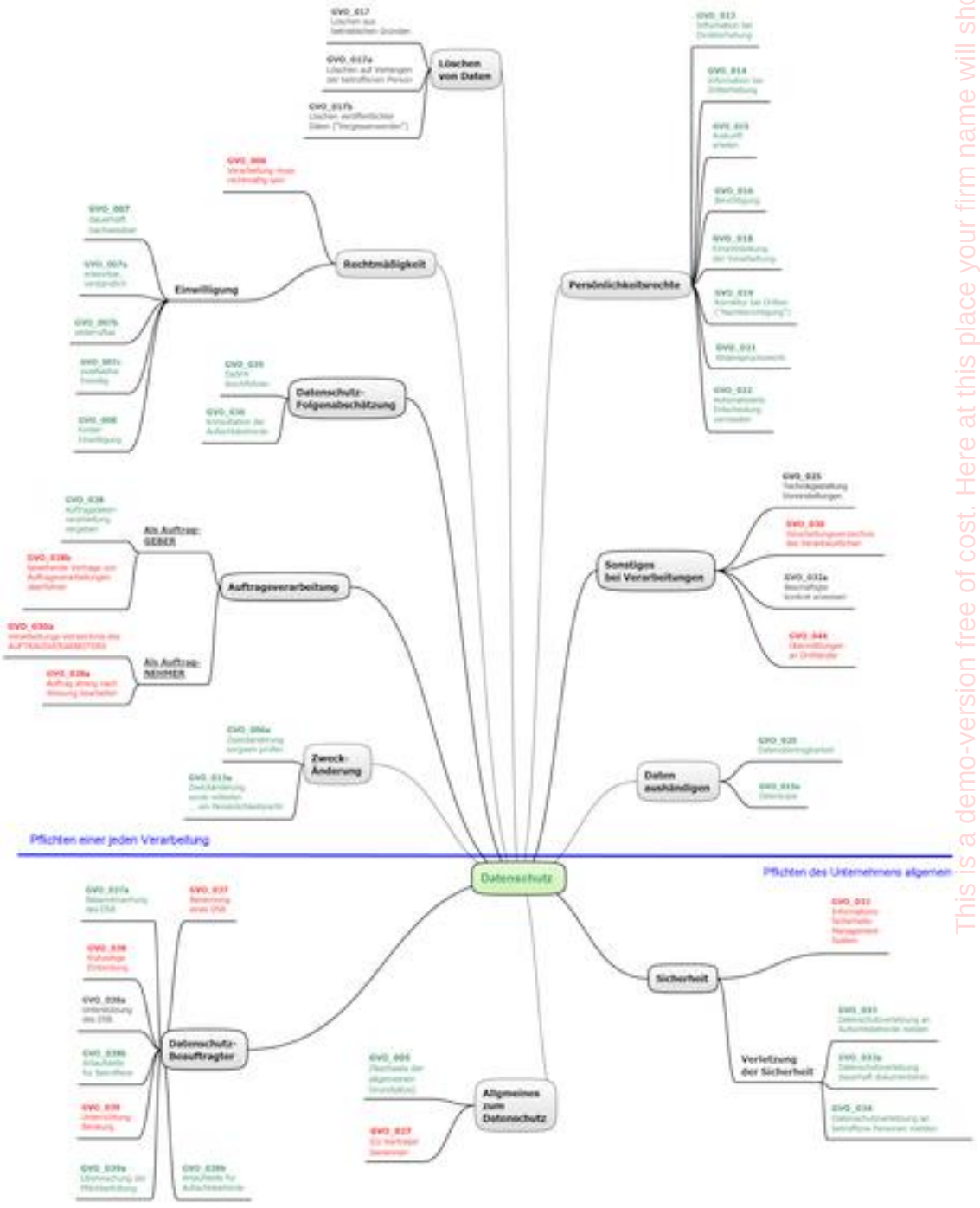
14.5 Mind map of obligations

Annex

The following mindmap illustrates the obligations within the meaning of the chapter “Alignment with obligations (Step 3)” on page 11.

All obligations of the GDPR are met (the obligations of the amended BDSG are omitted to make it clearer). The obligations above the blue line affect every individual process; the obligations below it are general obligations. The obligations in red must be tackled immediately; the obligations in black can wait until 25/05/2018; the obligations in green are only relevant after 25/05/2018 (but must be prepared before this of course).

A high-quality version of the mindmap can be found in the file **PrivazyPlan.zip** (see page 26) in the subdirectory “_Allgemeines” (General).



Source: PrivazyPlanMindmap_demo.png

14.6 Index

Annex

You can find the most important terms here in the index to easier locate them in the text.

For technical reasons, the page numbers do not serve as hyperlinks that take you directly to the desired page. You can jump to the desired page by pressing "Ctrl + G" when you are in the PDF reader window.

Any terms relating to the Federal Data Protection Act are designated by the suffix "(DE)".

E

F

G

I

J

L

M

O

P

R

S

T

V

W