Expert Opinion

on amendments to the status of the Data Protection Officer due to the General Data Protection Regulation

on behalf of the

Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.
[Professional Association of Data Protection Officers of Germany (BvD) e.V.]
Budapester Strasse 31
10787 Berlin

compiled by

Derra, Meyer & Partner Rechtsanwälte PartGmbB

in cooperation with the lawyers

Stefan Eßer
Konrad Menz
Prof. Dr. jur. Jürgen Meyer
Christiane Schrader-Kurz
Nils Steffen

www.derra.eu

Foreword

The following expert opinion (hereinafter referred to as "expert opinion") is based on the framework conditions that were defined when the expert opinion was commissioned on 27 February 2017. In several discussions with the client, the content of these conditions has been supplemented with regard to the structure of the expert opinion.

In accordance with the task commissioned, the authors of the expert opinion only answered the questions posed by the Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. *[Professional Association of Data Protection Officers of Germany]*. Therefore, consequential considerations directly or indirectly connected with the questions were not addressed.

The compilation is based on the General Data Protection Regulation which entered into force on 25 May 2016 and is directly applicable from 25 May 2018 and the Data Protection Adaptation and Implementation Act (DSAnpUG-EU; hereinafter referred to as "Adaptation Act") passed by the Federal Council (and previously by the Bundestag *[German parliament]*) on 12 May 2017. Article 1 of the Adaptation Act (AnpassungsG) passed a new Federal Data Protection Act (BDSG) (hereinafter referred to as “BDSG-new”), even though the EU Commission had criticised the previous draft of the EU Adaptation Act (DSAnpUG-EU). The BDSG-new will enter into force on 25 May 2018 after it has been signed by the Federal President and published in the Federal Law Gazette.

The Federal Data Protection Act in its current version is abbreviated in this expert opinion to “BDSG” without any addition.

This expert opinion is based on the legal situation as of 30 June 2017 as well as the case law and literature published up to this date. A change in the legal situation or judicial rulings may necessitate a different assessment in the future. Literature on the new developments and changes associated with the General Data Protection Regulation is only just beginning to emerge to a certain extent and the legal issues raised in this expert opinion must be examined in a differentiated manner. A conclusive and all-encompassing answer to the legal questions contained in this expert opinion cannot therefore be guaranteed.

The expert opinion refers exclusively to data protection officers in the non-public sector. In the following, the term "data protection officer" is considered gender neutral. The male pronoun is used throughout in the interests of easier readability.

On these premises, the structural organisation of this expert opinion is presented as follows:

- Table of contents
- Bibliography
- Practice-oriented summary of key findings
- Detailed answering of the defined questions
- Appendixes (recommendations for action, sample appointment certificate (old), sample consultancy agreement (old)

TABLE OF CONTENTS

Foreword 2

Table of contents 3

Bibliography 7

Summary of key findings 10

Expert opinion

1. Status of the data protection officer in the GDPR from a labour law perspective 11

1.1 Labour law evaluation of old cases in relation to internal data protection officers 11

1.1.1 Question: "Does an appointment made before the GDPR entered into force automatically end when the GDPR becomes effective?" 12

1.1.2 Question: "Does employment that was in place before the GDPR came into force automatically end when the GDPR becomes effective?" 14

1.1.3 Question: "Does the existing protection against dismissal for old cases pursuant to the BDSG continue to exist under the GDPR or do only the new provisions of the GDPR apply?" 15

1.1.3.1 Question: "Can it be assumed that the old BDSG regulation has been "incorporated" into the contract when an appointment is made during the validity of the BDSG, so that the old legal protection continues to exist contractually, even if the BDSG regulation is no longer applicable." 19

1.1.4 Question: "Does the entry into force of the GDPR provide grounds for revocation" 20

1.1.4.1 Question: "... if the GDPR no longer requires a designation?" 20

1.1.4.2 Question: "… even if the GDPR imposes a designation requirement?" 23

1.1.5 Question: "Does the entry into force of the GDPR provide extraordinary or ordinary grounds for termination of the employment relationship 24

1.1.5.1 Question: ".. if the GDPR no longer requires a designation?" 24

1.1.5.2 Question: "… even if the GDPR requires a designation?" 25

1.2 Contractual status of the external data protection officer in relation to appointments prior to the date of applicability of the GDPR 25

1.2.1 Question: "Does an appointment made before the GDPR entered into force automatically end when the GDPR becomes effective?" 26

1.2.2 Question: "Does the contracting of persons before the GDPR entered into force automatically end when the GDPR becomes effective? 28

1.2.3 Question: "Does the entry into force of the GDPR constitute grounds for revocation 29

1.2.3.1 Question: ... if the GDPR no longer requires a designation?" 29

1.2.3.2 Question: "… even if the GDPR requires a designation?" 29

1.2.4 Question: "Does the entry into force of the GDPR provide extraordinary or ordinary grounds for termination of the employment relationship 30

1.2.4.1 Question: "... if the GDPR no longer requires a designation?" 30

1.2.4.2 Question: "… even if the GDPR requires a designation?" 30

1.3 Protection of the appointed data protection officer pursuant to the GDPR 31

1.3.0 Foreword to 1.3.1: Basic principles of civil liability of the data protection officer

1.3.0.1 Liability of the data protection officer in the event of non-prevention of a data protection breach in the company 38

1.3.0.1.1 Monitoring system and system of action of the GDPR

1.3.0.1.2 Legal status of the data protection officer 43

1.3.0.1.3 "Monitoring" 44

1.3.0.2 Result

1.3.1 Question: "Under what conditions can the designated employed data protection officer be held liable? 46

1.3.2 Question: "Under what conditions can the external (contracted) designated data protection officer be held liable?" 51

1.3.3 Question: "The data protection officer is tasked with meeting compliance with the GDPR. Is liability conceivable in the event of sanctions due to insufficient monitoring? What are the conditions for this?" 53

1.3.4 Question: "Could contractual limitations of liability apply?" 55

1.4 Annex questions 56

1.4.1 Question: "Are there any differences between internal (employed) and external (see sample contract) data protection officers?" 57

1.4.2 Question: "Are implied appointments possible through continuing to perform the task?" 57

2. Criminal status of the data protection officer under the GDPR

2.1 Preliminary questions on the GDPR **58**

2.1.1 Question: “Does the data protection officer have a duty to inform himself of data protection-relevant processes?“ 58

2.1.2 Question: “Does the data protection officer have a duty to monitor, or even ensure, the implementation of his instructions/stipulations?” 59

2.1.3 Question: “Does the data protection officer have a duty to have a data protection organisation for his activities in addition to the one which the company (cf. Articles 5, 12, 24 GDPR) is required to set up.“ 60

2.2 Criminal liability **60**

2.2.1 Question: "Is it possible for the designated data protection officer to be held criminally liable?” 61

2.2.2 Question: "Is the designated data protection officer liable for penalties imposed by the GDPR? Which of his duties are penalised directly by the GDPR?“ 64

2.2.3 Question: “Is the designated data protection officer subject to a general duty to prevent infringements of data protection?“ 67

2.2.4 Question: “Does the designated data protection officer have a duty to prevent certain data protection breaches within the company?“ 68

2.2.5 Question: "Monitoring tasks are one of the main obligations formulated for data protection officers. Can direct penalties result from insufficient monitoring within the company?“ 68

2.2.6 Question: "Does the designated data protection officer have an obligation to prevent data protection breaches within the company if he previously drew attention to the unlawfulness?“ 69

2.2.7 Question: "Does it make a difference whether the data protection officer is an employee of the company or an external service provider?“ 69

2.3 Delegated tasks **69**

2.3.1 Question: "Where criminal liability is concerned, is a distinction made between the fundamental tasks of the data protection officer, on the one hand, and duties that are assumed by virtue of delegation, on the other?”

2.3.2 Question: “When does the data protection officer incur criminal liability for delegated tasks? Is the nature of the delegation of tasks relevant for this purpose?“ 70

Appendix 1 - Recommendations for action

Appendix 2 – Sample appointment certificate (old - not to be used)

Appendix 3 – Sample consultancy agreement (old - not to be used)

Bibliography

Albrecht, Jan Philipp; Jotzo, Florian, „Das neue Datenschutzrecht der EU“, publisher Nomos Verlagsgesellschaft, 2017

Behling, Thorsten, ZIP 2017, 697 - 706, „Die datenschutzrechtliche Compliance – Verantwortung der Geschäftsleitung"

Bergt, Matthias in: Kühling, Jürgen (Pub.); Buchner, Benedikt (Pub.), „Datenschutz-Grundverordnung: DS-GVO“, publisher C.H. Beck OHG, 2017

Bongers, Frank; Krupna, Karsten, ZD 2013, 594 - 599, „Haftungsrisiken des internen Datenschutzbeauftragten – Zivilrechtliche Haftung, Bußgelder und Strafen".

Eisele, Jörg in: Rotsch, Thomas (Ed.), Criminal Compliance, publisher Nomos Verlagsgesellschaft, 2015

Ettig, Diana; Bausewein, Christoph in: Wybitul, Tim (Pub.), Handbuch EU-Datenschutz-Grundverordnung, Fachmedien Recht und Wirtschaft, 2017

Franzen, Martin in: Müller-Glöge, Rudi (Pub.); Preis, Ulrich (Pub.); Schmidt, Ingrid (Pub.), Erfurter Kommentar zum Arbeitsrecht, 17th Edition, publisher C.H. Beck OHG, 2017

Gola, Peter; Brink, Stefan in Boecken, Winfried (ed.); Düwell, Franz Josef (ed.); Diller, Martin (Pub.); Hanau, Hans (Pub.), Gesamtes Arbeitsrecht, Volume 1, publisher Nomos Verlagsgesellschaft, 2016

Gola, Peter; Klug, Christoph; Körffer, Barbara in: BDSG: Bundesdatenschutzgesetz Kommentar, 12th edition, Verlag C.H. Beck OHG, 2015

Gola, Peter; Klug, Christoph, NJW 2007, 118 - 122, „Neuregelungen zur Bestellung betrieblicher Datenschutzbeauftragter“

Grüneberg, Christian in Palandt – Bürgerliches Gesetzbuch, 76th Edition, publisher C.H. Beck OHG, 2017

Hamann, Christian, BB 2017, 1090 - 1097, „Europäische Datenschutz-Grundverordnung – neue Organisationspflichten für Unternehmen“.

Heberlein, Horst in: Ehmann, Eugen (ed.); Selmayr, Martin (Pub.), DS-GVO - Datenschutz-Grundverordnung, publisher C.H. Beck OHG, 2017

Heermann, Peter W. in: Henssler, Martin (Ed.), Münchener Kommentar zum BGB, Volume 6, 6th Edition, publisher C.H. Beck OHG, 2012

Herbst, Tobias in: Kühling, Jürgen (Pub.); Buchner, Benedikt (Pub.), Datenschutz-Grundverordnung: DS-GVO, publisher C.H. Beck OHG, 2017

Hesse, Dirk in: Henssler, Martin (Ed.), Münchener Kommentar zum BGB, Volume 6, 6th Edition, publisher C.H. Beck OHG, 2012

Jaspers, Andreas; Reif, Yvette, RDV 2016, 61 - 68, „Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben"

Klug, Christoph, ZD 2016, 315 - 319, „Der Datenschutzbeauftragte in der EU Ma0gaben der Datenschutzgrundverordnung"

Kort, Michael, ZD 2017, 3 - 6, „Was ändert sich für Datenschutzbeauftragte, Aufsichtsbehörden und Betriebsrat mit der DS-GVO? Die zukünftige Rolle der Institutionen rund um den Beschäftigtendatenschutz".

Kühling, Jürgen; Martini, Mario, EuZW 2016, 448 - 454, „Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?"

Lepperhoff, Niels; Müthlein, Thomas, Leitfaden zur Datenschutz-Grundverordnung, Datakontext, 2017

Marschall, Kevin, ZD 2014, 66 - 71, „Strafrechtliche Haftungsrisiken des betrieblichen Datenschutzbeauftragten? Notwendige Handlungsempfehlungen"

Marschall, Kevin; Müller, Pinkas, ZD 2016, 415 - 420, „Der Datenschutzbeauftragte im Unternehmen zwischen BDSG und DS-GVO - Bestellung, Rolle, Aufgaben und Anforderungen im Fokus europäischer Veränderungen"

Nemitz, Paul in: Ehmann, Eugen (Pub.); Selmayr, Martin (Pub.), DS-GVO - Datenschutz-Grundverordnung, publisher C.H. Beck OHG, 2017

Oetker, Hartmut in: Krüger, Wolfgang (Red.), Münchener Kommentar zum BGB, Volume 2, 6th Edition, publisher C.H. Beck OHG, 2016

Paal, Boris P. (Pub.); Pauly, Daniel (Pub.), General Data Protection Regulation: GDPR, publisher C.H. Beck OHG, 2017

Piltz, Carlo, K&R 2016, 709 - 715, "„Die Datenschutz-Grundverordnung – Teil 3: Rechte und Pflichten des Verantwortlichen und Auftragsverarbeiters".

Roßnagel, Alexander, MMR 2015, 359 - 264, „Der Anwendungsvorrang der eIDAS-Verordnung - Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?"

Sachs, Andreas; Kranig, Thomas; Gierschmann, Markus, Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden, publisher Bundesanzeiger Verlag, 2017

Schantz, Peter, NJW 2016, 1841 - 1847, „Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht"

Schneider, Jochen, Datenschutz nach der Datenschutz-Grundverordnung, publisher C.H. Beck OHG, 2017

Simitis, Spiros (Pub.), Bundesdatenschutzgesetz, 8th Edition, publisher Nomos Verlagsgesellschaft, 2014

Thode, Jan-Christoph, CR 2016, 714 - 721, „Die neuen Compliance-Pflichten nach der Datenschutz-Grundverordnung“

Von dem Bussche, Axel Freiherr in: Plath, Kai-Uwe (Pub.), BDSG DS-GVO: Kommentar zum BDSG und zur DSGVO sowie den Danteschutzbestimmungen des TMG und TKG, 2nd Edition, publisher Dr. Otto Schmidt, 2016

Wybitul, Tim, CCZ 2016, 194 - 198, „Welche Folgen hat die EU-Datenschutz-Grundverordnung für Compliance?“

Summary of the main findings:

- Data protection officers appointed under the current Federal Data Protection Act remain in office even after the General Data Protection Regulation has come into effect. The appointments remain effective as designations; however, as of 25 May 2018, the General Data Protection Regulation is directly applicable.

- Nor do the employment contracts of the internal data protection officers automatically end when the General Data Protection Regulation enters into force.

- The requirements for the mandatory appointment of a data protection officer and also for protection against dismissal and discrimination are regulated differently in the General Data Protection Regulation than in the currently applicable Federal Data Protection Act, which will no longer be applicable once the General Data Protection Regulation becomes effective. However, the provisions on protection against dismissal and compulsory appointment will largely be retained in a form adapted to the General Data Protection Regulation following the adoption of BDSG-new.

- Neither the appointment or designation of the external data protection officer nor his appointment shall end automatically because this is not provided for by law or in the sample contract submitted.

- The data protection officer has no general duty to prevent breaches of data protection within the company. He monitors the company's organisational structure under data protection law and reports his findings to senior management. The intensity of his reporting must follow a risk-based approach. Active intervention to eliminate or prevent individual infringements, however, is not the responsibility of the data protection officer in the absence of appropriate authority to issue directives.

- The external data protection officer is not liable for every breach of data protection in the company. In accordance with general principles of civil law, he is liable for culpable breaches of an obligation without benefitting from liability privileges - as is the case with an internal data protection officer.

- There is no direct responsibility under sanctions law for the data protection officer pursuant to Article 83 GDPR. A responsibility of this nature also does not result from an affirmative obligation in the context of an assignment (differently than for the Compliance Officer), provided that his tasks are orientated along the lines of the original specifications of the General Data Protection Regulation. However, an affirmative obligation may arise if the data protection officer is delegated further duties and powers.

1. Status of the data protection officer pursuant to the GDPR from the point of view of labour law

Explanation of the questioner: *"In the case of internal data protection officers, a distinction may have to be made between the employment relationship and the appointment as company data protection officer. It should also be borne in mind that internal data protection officers - i.e. salaried employees - often spend only part of their working time on their activities as data protection officers and, in addition, perform (mainly) other tasks in the company than salaried employees".*

1.1 Labour law evaluation of old cases in relation to the internal data protection officer

In the course of preparing this expert opinion, we first examined what consequences the entry into force of the General Data Protection Regulation (GDPR) will have for internal data protection officers already appointed at the time of its entry into force. Internal data protection officers are those data protection officers who are employed by a company. According to the settled case law of the Federal Labour Court, they are generally to be regarded as employees.[1] The company data protection officer is a core element of the General Data Protection Regulation.[2]

Furthermore, in accordance with the provisions of the currently applicable Federal Data Protection Act (BDSG) and also in accordance with the provisions of the General Data Protection Regulation and the DSAnpUG-EU passed by the Bundesrat *[upper house of Federal parliament]* (and previously by the Bundestag *[Federal parliament]*) on 12 May 2017, a distinction must be made between the basic relationship and the appointment relationship in the activities of the data protection officer. The Adaptation Act passed the BDSG-new, which will replace the BDSG and contain the relevant national regulations on data protection officers. The unilateral appointment of a data protection officer must be separated from the contractual basis on the basis of which the data protection officer is obligated by law to assume the task of data protection officer. In the case of an employee, the basic relationship is usually an employment relationship. If the employee agrees to his appointment, the rights and obligations under the employment contract expand with the appointment for the period for which he is appointed. Nevertheless, a distinction must be made between the two legal relationships.[3]

The General Data Protection Regulation entered into force on 25 May 2016, the 20th day after its publication in the Official Journal of the European Union (Article 99(1) GDPR). However, it only applies after 2 years have passed since it entered into force, i.e. from 25 May 2018 (Article 99(2) GDPR). The comments in this expert opinion concern the legal situation with regard to the General Data Protection Regulation as of the date of applicability of the General Data Protection Regulation.

[1] Franzen in Erfurter Kommentar zum Arbeitsrecht *[Erfurt commentary on labour law],* 17th edition 2017, Article 4 f BDSG, marginal 8
[2] Heberlein in Ehmann/Selmayr, Datenschutz-Grundverordnung *[General Data Protection Regulation]*, 2017, Article 37 marginal 1
[3] so already BAG, ruling dated 13 March 2007 - 9 AZR 612/05

1.1.1 **Question:** *"Does an appointment made before the entry into force of the General Data Protection Regulation automatically end with the entry into force of the General Data Protection Regulation?*

The General Data Protection Regulation also places the legal entity of the data protection officer, which has so far found its legal basis in Article 4 f BDSG, on a new legal basis. With the General Data Protection Regulation, the European legislator has adapted the data protection officer, who has been mainly known in Germany to date, and decided that a data protection officer must be appointed under the conditions of Article 37(1) GDPR. According to the recitals to the Regulation, 'the controller or processor should be assisted in monitoring internal compliance with the provisions of this Regulation by another person with expertise in the field of data protection law and procedures.'[4]

According to Article 288(2) sentence 1 of the Treaty on the Functioning of the European Union (TFEU), an EU regulation has general validity. This means that it is directly applicable and has direct legal effects. Pursuant to Article 288(2) sentence 2 TFEU, it is binding in all its parts without the need for a national act of transposition in each Member State. A European regulation is therefore directly binding on Union citizens and public authorities.[5]

If there is a contradiction between the national laws of the individual member states and the provisions of an EU regulation, the EU regulation takes precedence. The respective national laws are not ineffective. However, the EU regulation is applied as a matter of priority. The national regulation that contradicts it - for example a German law - may not be applied. Application precedence is an "unwritten norm of primary Union law."[6]

Against the background of the significance and regulatory effect of an EU regulation outlined above, it must therefore be examined whether the entry into force of the General Data Protection Regulation will lead to the legal concept of the data protection officer being placed on a new basis in such a way that, from the entry into force of the General Data Protection Regulation, all offices of data protection officers appointed on the basis of Article 4 f BDSG will have to end. If necessary, the offices of data protection officers could also end for only a so-called "legal second" and then "resume" under the conditions of the General Data Protection Regulation and the BDSG-new.

The legal classification of the appointment of the data protection officer is essential for answering the question. The Federal Data Protection Act has always used the term "appoint" (“Bestellung”) to designate a data protection officer in a company or enterprise. The BDSG-new, on the other hand, in Article 5(1) and Article 38(1) respectively, speaks of the "designation" (“Benennung”) of the data protection officer. In this respect, its terminology corresponds to that of the General Data Protection Regulation, which also does not refer to the appointment but to the designation of the data protection officer (Article 37(1) GDPR). Despite the different terms, however, it can be assumed that the term "designation" under

[4] Recital 97 to Regulation EU 2016/679
[5] Roßnagel, MMR 2015, 359
[6] Roßnagel, loc. cit.; BVerfG, ruling of 22.10.1986 - 2 BvR 197/83

European law corresponds to the term "appointment" previously used in Germany. In any case, the jurisprudence and literature consulted by the authors of this expert opinion do not contain any opinion that should be understood as meaning that the designation of the data protection officer constitutes a different legal act from the hitherto customary appointment. On the contrary, as a rule there is no differentiation between the two terms. Both terms are often used congruently.[7]

As an interim result, it should therefore be noted that the amended terminology of the General Data Protection Regulation and the BDSG-new does not mean that an appointment as such should no longer be valid on the basis of the directly applicable General Data Protection Regulation.

In the opinion of the authors of this expert opinion, the change in the legal basis for the appointment/designation of the data protection officer should not result in an automatic termination of the appointments made under the currently applicable Federal Data Protection Act. This is supported in particular by the fact that the automatic termination of the office of Data Protection Officer is so far completely unknown. Even in the event that the statutory requirement of a compulsory appointment is abolished, the relevant literature in this respect assumes that there is only one reason for the dismissal of the data protection officer, but not a termination of office by operation of law. Even under the application of the BDSG, an explicit revocation was required both to clarify the labour law situation and to clarify the status of the data protection officer. Such a declaration by the employer might also be necessary in the future, because a "voluntary" appointment/designation of a data protection officer is always possible.[8] This assessment is not changed by the case-law on the termination of the office of data protection officer in the event of a transfer of business pursuant to Article 613a BGB9. The transfer of a business represents a special case in which employment relationships are transferred to a new owner of the business for legal reasons without the need for an express agreement between the employees and the purchaser of the business. It cannot be compared with the constellation of a change in the legal basis to be examined here.

In contrast to Article 4 f (1) BDSG, the General Data Protection Regulation and the BDSG-new (Articles 5, 38) do not provide for any formal requirement for the appointment of the data protection officer. In future, the appointment of the data protection officer can also be made orally; written form is no longer required. However, for reasons of legal certainty, it is strongly recommended that appointments continue to be made in writing.[10]

---

[7] Thus, von dem Bussche speaks in Plath BDSG GDPR, 2nd edition, Article 37(2), of an obligation to appoint also with regard to the General Data Protection Regulation

[8] Gola/Klug, NYW 2007, 118, 119

[9] LAG Berlin-Brandenburg, ruling of 15.10.2013 - 3 Sa 567/14

[10] Heberlein in Ehmann/Selmayr, loc. cit., Article 37, marginal 17; Lepperhoff/Müthlein, Leitfaden zur DS-GVO *[Guide to the GDPR],* 2017, p. 82

For the designation, it remains the case at any rate that a designation act of any kind must take place, especially since Article 37(7) GDPR provides that the data controller or the processor must publish the contact data of the data protection officer and communicate this data to the supervisory authority.

The fact that the General Data Protection Regulation in Article 38(3) explicitly departs from a "dismissal" – or revocation - the legal opinion expressed by the authors of this expert opinion corresponds to the fact that an automatic end to the office of data protection officer should not be brought about by the effectiveness and entry into force of the General Data Protection Regulation. According to the wording of Article 38(3) GDPR, the European legislator itself assumes that the office of the designated data protection officer must be terminated by a further legal act of the controller, namely dismissal.

Mirroring the requirement of designation, the requirement of revocation of the designation (dismissal) will continue to apply in the future. In the opinion of the authors of this expert opinion, an "automatic" end of the office of data protection officer cannot be justified by legal dogma. However, it should be pointed out that - also inversely to the no longer existing formal requirement for the appointment - the dismissal of the data protection officer can in future take place informally, i.e. including in an unwritten form. As a rule, the controller will prefer to carry out a dismissal in writing in order to be able to prove this if necessary. It is also conceivable, however, that a verbal dismissal may take place in the presence of witnesses. In this respect, it is also advisable for dismissal for reasons of legal certainty to contractually agree to a written form as a formal requirement between the controller and the data protection officer.

A corresponding notification to the supervisory authority must in any case be made in addition; this results conversely from the disclosure requirement pursuant to Article 37(7) GDPR.

On the basis of the above, the answer to the question must therefore be that an appointment made before the entry into force of the General Data Protection Regulation does not automatically end with the entry into force/effectiveness of the General Data Protection Regulation.

1.1.2 Question: *"Does an appointment made before the entry into force of the General Data Protection Regulation automatically end when the General Data Protection Regulation comes into effect*?

An essential basic principle of German labour law is that a work or employment relationship cannot end automatically. An exception in this context is an effectively fixed-term employment relationship which ends merely through the passage of time. All other (open-ended) employment relationships end exclusively through giving notice or concluding a dissolution contract.

According to Article 623 BGB *[German Civil Code]* the termination of employment relationships by termination or dissolution contract also requires the written form to be effective.

An automatic termination of the employment relationship of a data protection officer with the entry into force of the General Data Protection Regulation is thus excluded in principle.

The regulation of Article 623 BGB *[German Civil Code]* is also not affected or inapplicable by the regulations of the data protection basic regulation. Despite the above-mentioned priority application of the provisions of an EU regulation, it should be noted that legislative competence in the field of labour law lies exclusively with the member states. Article 623 of the German Civil Code (BGB) establishes a basic labour law principle in Germany. It is therefore excluded that this basic principle may be removed or not be applicable by the rules of the General Data Protection Regulation.

It should also be noted that the wording of the General Data Protection Regulation does not indicate that the labour law provisions of the individual Member States should not be applied to the employment relationships of the internal data protection officers. The basic Regulation on data protection does not contain any provisions on the employment relationships of data protection officers and is therefore in line with the provisions of the Treaty on the Functioning of the European Union (Articles 3 to 6 TFEU).

1.1.3 Question: *"Does the protection against dismissal existing under the BDSG for old cases also continue to apply under the GDPR or do only the new provisions of the GDPR apply*?

Also, for the purpose of answering this question, the "triad" to be noted between the Federal Data Protection Act in force at the time this expert opinion was prepared, the General Data Protection Regulation and the BDSG-new must be considered in this expert opinion.

The Federal Data Protection Act in its version valid at the time of the preparation of this expert opinion standardises the well-known far-reaching protection against dismissal for internal data protection officers. However, this protection against dismissal is only available to data protection officers for whom an obligation to appoint them exists (Article 4 f (3) S.5 BDSG). In particular, Article 4 f (3) BDSG provides for extremely extensive protection against dismissal and against disadvantageous measures by the employer compared to the rest of Europe. The provisions of Article 4 f (3) BDSG are - expressed in a generalized way - oriented along the protection of works councils in accordance with the Betriebsverfassungsgesetz (BetrVG) *[Works Constitution Act]*. In principle, an internal data protection officer is not bound by orders issued by the controlling body, i.e. usually the employer, as far as the exercise of the office of data protection officer is concerned. Furthermore, the data protection officer shall not be penalised due to the performance of his/her duties. The appointment of a data protection officer can be revoked in accordance with Article 626 BGB *[German Civil Code]*. The same applies to the termination of the employment relationship, which is also only permissible if evidence is present which entitles the controller to terminate the employment relationship for important reasons without observing a period of notice. After his dismissal as data protection officer, the data protection officer enjoys so-called

"follow-up" protection for one year against fair dismissal of the employment relationship.

On the other hand, the General Data Protection Regulation contains an initially much lower level of protection for the data protection officer in its wording. While German law has so far been characterised by the fact that the independence of the company data protection officer is guaranteed by the protection of his person, which is based on the protection of officers under works constitutional law such as works council members, this does not apply to the same extent in the General Data Protection Regulation. [11]

The provisions governing the protection of the data protection officer are to be found in the prescriptions of Article 38(3) GDPR. These state that the controller and the processor 'shall ensure that, in the performance of his duties, the data protection officer does not receive orders regarding the performance of those duties'. Furthermore, the data protection officer may not be dismissed or penalised by the controller "due to the performance of his duties".

It is true that the General Data Protection Regulation provides for safeguard mechanisms in Article 38 to ensure the independence of the company data protection officer, namely with regard to his freedom from orders and protection against dismissal. However, the General Data Protection Regulation does not contain any protection for the company data protection officer, with a view to guaranteeing his independence, comparable to the provisions of the currently applicable Federal Data Protection Act.[12] In particular, the pure wording of the General Data Protection Regulation does not include any protection against dismissal of the data protection officer.

As stated above, the General Data Protection Regulation, as an EU Regulation within the meaning of Article 288 TFEU, takes precedence over national law.

The competence of the European Union to adopt the General Data Protection Regulation derives in particular from Article 16 TFEU. Pursuant to Article 16(2) TFEU, the European Parliament and Council, acting in accordance with the ordinary legislative procedure, shall adopt provisions on the protection of individuals with regard to the processing of personal data by the institutions, bodies, offices and agencies of the Union and by the Member States in the exercise of activities within the scope of Union law and on the free movement of such data. In view of the fact that the competence to legislate in the area of labour law lies exclusively with the member states on the basis of the provisions of the treaties of the European Union, in particular the TFEU, one could consider whether the extensive protection of data protection officers against dismissal under the currently applicable Federal Data Protection Act can be eliminated at all by the provisions of the General Data Protection Regulation. In this context, however, it should be noted that the legal concept of the data protection officer clearly falls

[11] Kort, ZD 2017, 3
[12] Cort, loc. cit.

within the legislative competence of the European Union under Article 16 TFEU. Accordingly, the European Union's legislative competence ought to also cover essential provisions relating to his tasks and position. Otherwise, it would hardly be possible for the European Union to legislate in a structured and complete manner in the individual thematic areas assigned to it. It should also be borne in mind that the protection of the data protection officer does not exist for its own sake, but serves to achieve and safeguard the respective purposes of the statutory provisions both under the provisions of the Federal Data Protection Act and under the provisions of the General Data Protection Regulation.[13]

With the BDSG-new, the German legislator has passed a new legal regulation to adapt its national law to the requirements of the General Data Protection Regulation. The text of the law provides for protection exceeding that of the General Data Protection Regulation (Article 38) against recall and dismissal of the data protection officer, being very much based on the provisions of the currently applicable Federal Data Protection Act.

Article 6(4) BDSG-new provides that dismissal of the data protection officer is only permissible in corresponding application of Article 626 BGB. Termination of the employment relationship is inadmissible unless evidence exists which entitles the public sector body to terminate the employment relationship for an important reason without observing a period of notice. After the end of the task of data protection officer, it is inadmissible to terminate the employment relationship within one year unless the public body is entitled to terminate it for an important reason without observing a period of notice. Article 6(4) BDSG-new applies according to Article 38(2) BDSG-new to data protection officers of non-public bodies as well, but only if their designation is mandatory.

Compared to the provisions of the General Data Protection Regulation, BDSG-new therefore contains a clear augmentation of the protection of the data protection officer against recall and dismissal. In this respect, the German legislator seems to continue to make use of the possibility of aligning the protection of the company's data protection officer with works constitutional functionaries such as works council members.[14]

As an interim result, it should be noted that BDSG-new provides for protection of the data protection officer against recall and dismissal corresponding to that of the currently applicable Federal Data Protection Act.

However, the "new" protection against dismissal under BDSG-new will only apply from the date on which the new national statutory regulation comes into force (25 May 2018).

In this respect, it must be clarified how the changes to the statutory regulations are to be classified in regulatory and temporal terms. The following applies here:

[13] See also von dem Bussche in Plath, BDSG GDPR, 2nd edition, Article 38, marginal 9

[14] Kort ZD 2017, 3, 4

- Under the General Data Protection Regulation, a lower level of protection of the data protection officer against revocation and dismissal applies compared to the previous Federal Data Protection Act (Article 4 f BDSG). According to the provisions of the General Data Protection Regulation, the Data Protection Officer must not be penalised because of the conscientious performance of his duties under Article 38 GDPR. Also, a dismissal "for the performance of his duties" is not permitted. Conversely, it should be assumed that a dismissal or ordinary or extraordinary termination of the employment relationship of the internal data protection officer is fundamentally possible at any time for other reasons, such as economic or operational reasons.[15]

  Even if the purpose of Article 38 GDPR certainly requires protection against circumvention, i.e. the ineffectiveness of a dismissal or termination if other reasons are merely used as an excuse,[16] the wording of Article 38 GDPR, even with a far-reaching interpretation based on the meaning and purpose of the provision, constitutes significantly reduced protection against dismissal in comparison with the currently applicable Federal Data Protection Act. This applies from the time the General Data Protection Regulation becomes effective, so that operational dismissals of data protection officers due to the discontinuation of the requirement to designate them (also only after GDPR) would be conceivable. Here, however - and this will have to be explained in the following – it is essential for the purposes of a practice-relevant consideration that the BDSG-new is taken into account.

- According to the case law of the Federal Labour Court and the Federal Constitutional Court, there is no general principle according to which protection against dismissal once acquired in the past as a result of earlier statutory regulation must continue to apply in the future. Even constitutional principles or fundamental rights, such as the fundamental right to freedom of occupational freedom under Article 12 of the Basic Law or the general principle of equality before the law under Article 3 of the Basic Law, do not result in already appointed data protection officers enjoying a kind of "statutory follow-up" protection against dismissal according to the earlier or no longer applicable provisions of the Federal Data Protection Act due to the removal of protection against dismissal resulting from the introduction of the General Data Protection Regulation.[17]

- With the BDSG-new on 25 May 2018, the national German legislator will enact a legal regulation which will lead to protection against dismissal of the data protection officer that corresponds to that of the currently applicable Federal Data Protection Act. This is, moreover, also extremely welcome, since the ability of an employed data protection officer to perform tasks independently without orders is ultimately only constructively conceivable if the data protection officer enjoys extensive protection against dismissal. Similarly to the members of a works council, data protection officers must also assume functions in the company which, in individual cases, conflict with the direct interests of the employer.

[15] von den Bussche in Plath BDSG GDPR 2nd edition, Article 38, GDPR marginal 10
[16] von den Bussche, loc.cit.
[17] Cf. also BAG, judgement of 21.9.2006 - 2 AZR 840/05; BVerfG, ruling of 27.1.1998 - 1 BvL 15/87

Designated persons must therefore be protected from measures which could jeopardise the purpose of the rules laid down in the General Data Protection. In this respect, the activity of a data protection officer without comprehensive protection against dismissal is practically inconceivable. Practical considerations also support this view. The circumvention protection (see above), which is undoubtedly also required by the wording of the General Data Protection Regulation, can in practice be achieved most easily and unproblematically if there is still extensive protection against dismissal. This view is shared by the national legislator, even though there are occasionally voices that want to reduce the protection against dismissal of the BDSG-new and leave it at the pure wording of the General Data Protection Regulation.[18]

- The adopted provisions of Articles 5, 6, 38 BDSG-new will enter into force together with the entry into force of the General Data Protection Regulation on 25 May 2018. This means that the data protection officer will continue to be protected in the future in the same way as the protection against revocation and dismissal previously provided for under the Federal Data Protection Act. Even if one were to proceed from the construct of a so-called "legal second" occasionally used in legal doctrine, in which the old protection against unfair dismissal under the currently applicable Federal Data Protection Act would be dropped and the new one would come into force under the General Data Protection Regulation and the New Federal Data Protection Act, it would not be possible to assume that the protection against unfair dismissal for data protection officers already appointed under the currently applicable Federal Data Protection Act would be dropped even temporarily. Neither the fact that different terminology is used (designation instead of appointment) nor the fact that in a large number of employment contracts or appointment documents reference is made to the provisions of the currently applicable Federal Data Protection Act, in particular Article 4 f BDSG, change this.

On the basis of the above explanations, the question must therefore be answered in such a way that the protection against dismissal existing under the Federal Data Protection Act does not continue to apply for old cases under the General Data Protection Regulation. The General Data Protection Regulation contains its own protection regulations for the data protection officer, but no explicit protection against dismissal (Article 38 GDPR). With the BDSG-new, the German legislator will introduce more extensive protection against dismissal for data protection officers even under the validity of the General Data Protection Regulation. This will also apply to old cases.

1.1.3.1 Question: *"Can it be assumed in the case of an appointment during the validity of the BDSG that the old BDSG regulation has been "incorporated" into the contract, so that the old legal protection continues in the contract, even if the BDSG regulation is no longer applicable?*

In view of the above, a discussion on the inclusion of protection against unfair dismissal under the currently applicable Federal Data Protection Act on the basis of the BDSG-new should not be necessary in the context of a contractual agreement. Nevertheless, it should be pointed out

[18] BDA statement on the Adaptation Act-E dated 14.03.2017, page 7

here that the inclusion of legal provisions in the content of a contractual relationship, such as an employment contract, is only likely to have occurred in exceptional cases. For this would require an explicit agreement on the statutory termination provisions. References to statutory provisions, such as an agreement under which the employee is appointed as "data protection officer pursuant to Article 4 f BDSG", would not be sufficient for this purpose.

For the contractual agreement of protection against unfair dismissal resulting from the law, it must be clear from the contract itself that the protection against unfair dismissal provisions of Article 4 f (3) BDSG shall apply even if the law itself is no longer applicable. A mere reference to paragraphs or provisions is not sufficient. Rather, it must be clear that the protection against dismissal should always apply to the parties irrespective of the statutory provisions. Here it is therefore necessary for the parties to expressly agree to this in the text of the employment contract. Only in the rarest of cases is such an agreement between the parties likely to exist.

As already explained above, no constitutional principles or fundamental rights under the Basic Law result in an earlier protection against dismissal continuing to apply in the event of a new statutory provision.

There is no automatism according to which the original protection against dismissal under the Federal Data Protection Act continues to be effective as a contractually agreed right of dismissal in the data protection officer's contract. An 'incorporation' cannot be assumed as a rule.

1.1.4 Question: *"Does the entry into force of the General Data Protection Regulation constitute a reason for dismissal*

1.1.4.1 **Question:** *... if designating a DPO is no longer a requirement under GDPR?"*

The question as to whether the status of a data protection officer in terms of data protection law or labour law (more on this under 1.1.5) is changed or can be changed with the introduction of the General Data Protection Regulation by an act of the controller or the employer is also to be assessed in principle on the basis of the "triad" of the currently applicable Federal Data Protection Act, the General Data Protection Regulation and the recently adopted BDSG-new.

The authors of this expert opinion and probably also the predominant view in jurisprudence and doctrine assume that - if the requirements of Article 626 BGB are not fulfilled - a reason for the dismissal of a data protection officer can only be considered if the legal requirements for the mandatory appointment of a data protection officer have changed. It must therefore be possible to envisage a case in which, under the previous legal situation, there was a requirement to appoint a data protection officer, but in which this no longer exists as a result of the new legal situation, in particular the entry into force of the General Data Protection Regulation. In this respect, the prerequisites for the mandatory appointment of a data

protection officer under the General Data Protection Regulation in conjunction with the BDSG-new must first be set out.

For the sake of completeness, we would like to point out again here that the office of data protection officer depends on the appointment (in old terms) or designation (in new terms) of the respective data protection officer, both under the current legal situation and under the provisions of the General Data Protection Regulation. The same applies to the termination of office. As already explained above, the General Data Protection Regulation in its Article 38(3) also assumes that a data protection officer must be dismissed. The conceivable approach that the office of data protection officer would in practice be abolished by law if the conditions for the mandatory appointment of a data protection officer were to be removed as a result of a change in the law cannot be applicable in this respect.[19]

According to the regulation of the currently valid Federal Data Protection Act, the threshold for requiring companies to appoint an in-house data protection officer is set low (Article 4 f BDSG). It is sufficient that more than 9 persons are constantly engaged in automated data processing or have processing operations is done which is subject to prior checking.[20]

On the other hand, the General Data Protection Regulation initially changes the criteria for the requirement to appoint the company data protection officer in a not inconsiderable way. Instead of the threshold value provided for in the Federal Data Protection Act for instituting the requirement to appoint a DPO where more than 9 persons in the company are permanently employed in automated data processing in the company, the provision in Article 37(1) GDPR now takes effect. Accordingly, a requirement to appoint a company data protection officer initially only exists if the company pursues "core activities" with regard to data processing (Article 37(1) lit. b and lit. c General Data Protection Regulation).[21] A comprehensive requirement to appoint a data protection officer exists pursuant to Article 37(1) lit. a General Data Protection Regulation only for the processing of data by an authority or a public body with the exception of courts which act within the scope of their judicial activity.

In contrast to the currently applicable Federal Data Protection Act, the General Data Protection Regulation thus pursues a purely risk-related approach.[22] It does not depend on the scope of data processing and, in particular, on how many persons in the company are involved in data processing. Due to the different approaches of the Federal Data Protection Act and the General Data Protection Regulation, the authors of this expert opinion believe that it is quite obvious that a practicable regulation is needed to clarify the legal situation and the requirements for the appointment of a data protection officer. This possibility is in fact also provided for in the General Data Protection Regulation (Article 37 (4) GDPR), and the German legislator has made use of it in the BDSG-new.

[19] LAG Berlin-Brandenburg, judgement dated 15.10.2013 - 3 Sa 567/14, according to this party's assessment, supports this legal view because the status of the data protection officer there is also linked to an appointment act by the controller/employer (see No. 36 of the reasons for the judgment).
[20] Kort ZD 2017, 3
[21] Heberlein in Ehmann/Selmayr, loc. cit., Article 37, marginal 10
[22] Schneider, (Datenschutz nach der Datenschutz-Grundverordnung) Data Protection according to the General Data Protection Regulation, p. 190

The fact that Article 37(4) of the General Data Protection Regulation expressly grants national legislators the right to independently define the conditions for the requirement to appoint a data protection officer has made it unnecessary in the legal discussion to clarify whether an extension or redefinition of the conditions of the requirement to appoint a DPO may be permissible on the basis of the priority of application of the EU Regulation. Nevertheless, it must be examined whether the provisions of the BDSG-new are consistent with those of the General Data Protection Regulation. This is because the provisions of the BDSG-new should not be applied if they contradict the provisions of the General Data Protection Regulation, whereby this assessment must always be viewed against the background of the authorisation basis in Article 37(4) GDPR.

The authors of this expert opinion do not assume that the provisions of the BDSG-new contradict the provisions of the General Data Protection Regulation. It is true that the provisions of the currently applicable Federal Data Protection Act could not simply be incorporated into the BDSG-new because harmonisation of the provisions is urgently required (see above). Nevertheless, with the BDSG-new, the German legislator has made the attempt to move away from the difficult-to-handle criteria for the requirement to appoint a DPO under Article 37 (1) (b) and (c) of the GDPR, which is ultimately to be welcomed in the interests of legal clarity.

According to the regulations of the BDSG-new for non-public companies (Article 38(1) BDSG-new) the controller and the processor appoint a data protection officer if they normally employ at least 10 persons permanently with the automated processing of personal data. If the controller or processor carries out processing operations which are subject to a data protection impact assessment pursuant to Article 35 GDPR, or if they process personal data commercially for the purposes of transfer, anonymised transfer or for the purposes of market or opinion research, they must appoint a data protection officer irrespective of the number of persons involved in the processing. The wording of the BDSG-new therefore ultimately corresponds to the previous provisions of the Federal Data Protection Act. The threshold value for staff involved in the processing of personal data is still 10, despite the slight change in the wording.

For the sake of clarification, it should be noted that the authors of this expert opinion believe that the term 'employment' should not be understood in the sense of employment under social insurance law. The threshold value is therefore reached if at all a number of persons who reach the threshold value are involved in data processing, regardless of their social security classification.

Instead of the prior check mentioned in the currently applicable Federal Data Protection Act, the BDSG-new provides for a requirement to appoint a data protection officer for processing operations that are subject to a data protection impact assessment pursuant to Article 35 GDPR. This in itself is system-compatible. Prior checking has been replaced in the General Data Protection Regulation by the data protection impact assessment pursuant to Article 35 GDPR.

The consequence of the provisions of the BDSG-new, which the authors of this expert opinion believe are to be applied in full in this respect is likely to be that a case constellation in which a data protection officer had to be appointed as obligatory under previous law in which this obligation is now removed by the new law, is hardly conceivable. Article 38(1) BDSG-new ties in with the provisions of the Federal Data Protection Act. Article 37(1) (b) and (c) of the GDPR contains additional provisions which may well raise questions in the future as to whether the provisions of the General Data Protection Regulation will result in even more extensive appointment obligations than hitherto. However, the requirements for the data protection officers already appointed under the validity of the previous law have not changed. Therefore, there should be no reason to dismiss a data protection officer on the basis of the new legal situation.

The question must therefore be answered to the effect that the new legal situation does not imply any reduction in designation obligations after the entry into force of the General Data Protection Regulation and the BDSG-new. In this respect, the entry into force and coming into effect of the General Data Protection Regulation does not constitute a reason for the dismissal of a data protection officer.

If, however, the BDSG-new version does not enter into force in its current version, it is quite conceivable that there could be cases in which a reason for dismissal could exist if the previous prerequisites for a compulsory appointment no longer apply.

1.1.4.2 Question: *"... even if there is a designation requirement under the GDPR?*"

This question must be answered in the same way as the previous one, with the proviso, however, that even in the absence of BDSG-new, the entry into force of the General Data Protection Regulation could not constitute a reason for the dismissal of a data protection officer, if he is also subject to an appointment requirement under the provisions of the General Data Protection Regulation.

At this point, it would be conceivable at best to have a theoretical discussion on the question of whether the entry into force of the General Data Protection Regulation and the BDSG-new could, for a "logical moment", lead to the elimination of the prerequisites for the mandatory appointment of a data protection officer or even to the removal of the legal basis for data protection officers who have already been appointed. Ultimately, it is inconceivable for the authors of this expert opinion that the change in the legal basis alone would mean that all the basic requirements for data protection officers already appointed could be eliminated. In particular, this would not be consistent with the spirit and purpose of the General Data Protection Regulation. The main objective of the General Data Protection Regulation is to protect data subjects from improper and unjustified processing of their data. If one were to grant controllers a right to extraordinary dismissal of data protection officers appointed in accordance with old law solely on the basis of the fact that the legal basis for the legal concept of the data protection officer henceforth results primarily from the General Data Protection Regulation, this objective would be jeopardised to a high degree.

1.1.5 **Question:** *"Does the entry into force of the General Data Protection Regulation constitute an extraordinary or ordinary reason for termination of the employment relationship*

1.1.5.1 Question: *... if under the GDPR there is no longer a requirement to designate a DPO*"?

It has already been stated in the context of this expert opinion that the entry into force of the General Data Protection Regulation on the basis of the provisions of Article 623 of the German Civil Code (BGB) cannot in any case lead to an "automatic" end to the employment or employment relationship of an employed data protection officer (1.1.2). Even the status relationship, which must be strictly separated from the employment relationship of the internal data protection officer, does not end automatically or on the basis of a statutory regulation, but always only on the basis of a unilateral act, namely the dismissal of the data protection officer (cf. Article 38(3) sentence 2 GDPR), both under the previous legal situation and under the provisions of the General Data Protection Regulation.

Assuming that the BDSG-new will come into force on 25 May 2018, the authors of this expert opinion do not believe that a case constellation is conceivable in which, under current law, there is an obligation to appoint a DPO which would no longer apply due to the new legal situation. An existing right of termination due to the entry into force of the General Data Protection Regulation could at most be justified by the fact that there is a case in which the new legal situation would no longer require an appointment or a designation. However, due to the BDSG-new legislation presented by the German legislator, this is hardly conceivable, as has already been stated several times. For these reasons, the entry into force of the General Data Protection Regulation will not constitute extraordinary or ordinary grounds for terminating the employment of the internal data protection officer, if the General Data Protection Regulation no longer requires the appointment of a data protection officer.

Analogous to the above remarks under 1.1.3, however, it should be pointed out that a termination of the employment relationship of the data protection officer for economic or operational reasons could certainly be considered if the BDSG-new should unexpectedly not enter into force and if the General Data Protection Regulation no longer requires an appointment.

However, a distinction should be made here between data protection officers who are active as such throughout their working time and those who devote only part of their working time to their activities as data protection officers. In the case of data protection officers in full-time employment, it would be easier to justify dismissal for operational reasons if the obligation to appoint staff ceased to apply than in the case of part-time data protection officers, for whom it would still have to be explained in detail that their entire workplace has ceased to exist as a result of the legal change.

The question must therefore be answered in such a way that the entry into force of the General Data Protection Regulation does not constitute a reason for the ordinary or extraordinary dismissal of the data protection officer if the BDSG-new enters into force as expected.

Otherwise, due to the partial elimination of the obligation to designate a DPO, dismissals for operational reasons could well be pronounced.

1.1.5.2 Question: *"... even if there is a requirement to designate a DPO under the GDPR?*"

In order to avoid repetitions, reference is made to the above remarks, in particular under 1.1.5.1. It would be conceivable, if at all, that the entry into force of the General Data Protection Regulation would constitute a reason for the termination of the employment relationship of the internal data protection officer if, on the basis of the provisions of the General Data Protection Regulation in conjunction with the BDSG-new, a previously existing requirement to designate (or appoint) would be eliminated. However, as has already been pointed out several times, this cannot be assumed.

For this reason, the entry into force of the General Data Protection Regulation does not constitute an extraordinary or ordinary reason for the termination of the employment relationship of the internal data protection officer, even if there is a requirement to designate a GDO under the General Data Protection Regulation. A different assessment would not arise even if the BDSG-new did not enter into force.

1.2 Contractual position of the external data protection officer with regard to orders prior to the date of application of the GDPR

Explanation of the questioner: *"The customer provides an example of a typical contract for the appointment of an external - i.e. not employed - data protection officer. This example serves the writer as a reference for answering the questions.*"

External data protection officers are those data protection officers who do not work within a company themselves. In addition to the internal data protection officer, the General Data Protection Regulation also provides for the external data protection officer. This results from the wording of Article 37(6) GDPR. It states that the data protection officer may be an employee of the controller or of the processor *"or perform his duties on the basis of a service contract*".

When appointing a data protection officer, a distinction must be made between the basic relationship of the activity and the appointment relationship, as already explained in point 1.1.1. In contrast to an internal DPO, the basic relationship of an external DPO is the consultancy agreement. This is legally independent of the appointment.[23] This means that there are two different aspects to consider. These are, on the one hand, appointments according to the Federal Data Protection Act or designations according to the General Data Protection Regulation and, on the other hand, the civil law contract on which the appointment or designation is based. If there is only an appointment or designation of an external data protection officer, then a civil law consultancy agreement has nevertheless been tacitly

[23] Recital 97 GDPR (old version)

concluded. Conversely, however, the conclusion of the civil law consultancy agreement does not constitute an appointment or designation, as a separate act is always required for this. This applies even if a designation under the General Data Protection Regulation can already be made verbally.[24]

Under the Federal Data Protection Act, the performance of the duties of the company data protection officer was regarded as a paid agency service. A contract such as this is characterised by the fact that the service provider undertakes to carry out an independent activity of an economic nature in order to protect the financial interests of third parties.[25]

Although the General Data Protection Regulation, when appointing an external data protection officer, is based on the wording of a service contract, an agency agreement will nevertheless exist here. This results from the tasks of the external data protection officer. The tasks regulated in Article 39 GDPR describe an independent activity of an economic nature in the interests of a third party. Even after the General Data Protection Regulation has come into force, it remains the case that the provisions of Articles 675, 662 ff., 611 ff. of the German Civil Code (BGB) apply to the appointment of an external data protection officer. Nevertheless, it should be noted that the only necessary act is the appointment or designation of the data protection officer. There is much to suggest that the consent of the data protection officer to be appointed or designated is a necessary prerequisite for effectiveness.[26] In any case, it is advisable to obtain this.

1.2.1 Question: *"Does an appointment made before the entry into force of the General Data Protection Regulation automatically end when the General Data Protection Regulation comes into effect*?

It should be made clear in advance that the following remarks only apply if no modifications have been agreed in the basic relationship of the consultancy agreement. The following explanations therefore only apply if either no modifying consultancy agreement has been concluded or the model of a consultancy agreement provided has been used.

Regarding the question of whether an appointment made before the entry into force of the General Data Protection Regulation automatically ends when the General Data Protection Regulation comes into effect, reference can essentially be made to point 1.1.1 of this expert opinion, since the legal basis for the appointment of a company data protection officer is independent of whether he is an internal or external data protection officer. In both cases, the appointment is the legal act by which the position of the data protection officer is justified. In the legal assessment according to the above remarks, the changed terminology of referring to a designation instead of an appointment does not result in an appointment no longer being

[24] Jaspers/tire RDV 2016, 61, 62 f
[25] Heermann in MünchKomm BGB, 6th edition 2012, Article 675 marginal 3
[26] Thus, deriving from the written form requirement of the order, Simitis Federal Data Protection Act, 8th edition 2014, Article 4f Rd-No. 57.

valid and automatically ending on the basis of the directly applicable General Data Protection.

The Federal Data Protection Act, taking into account the prohibition of discrimination in conjunction with the freedom to issue orders pursuant to Article 4 f (3) sentences 2 and 3 BDSG, a general time limit on the appointment was largely rejected and the appointment was regarded as basically unlimited.[27]

According to the applicable provisions of the General Data Protection Regulation, the appointment of a data protection officer according to the provisions of the General Data Protection Regulation is also to be regarded as basically unlimited in time. In accordance with its wording in Article 37(6) GDPR, this provision assumes that the designation may already be based on an (unlimited) employment relationship. Although this does not exclude the possibility of a fixed-term appointment, it does, however, initially mean an unlimited appointment.[28]

In the opinion of the authors of this expert opinion, the appointment or designation of an external data protection officer does not lead to an automatic termination of the appointments made under the previous Federal Data Protection Act, since - as already explained - an automatic termination of the office of data protection officer is unknown in the statutory provisions. The Federal Data Protection Act did not provide for termination of the office by operation of law, nor does the General Data Protection Regulation, the Adaptation Act or the BDSG-new provide for such termination.

A different situation may apply if something to the contrary is contractually regulated. From the sample certificate of appointment provided concerning the appointment of an external data protection officer,[29] the appointment is a consequence of the agreements in the consultancy agreement and is to end automatically with the termination of this contract.[30] The provision is to be interpreted in such a way that no other automatic termination options agreed under civil law are provided for. Automatic termination of the appointment for any reasons other than termination of the underlying consultancy agreement is not apparent. The question of automatic termination of the assignment will be dealt with below under point 1.2.2.

An appointment made before the entry into force of the General Data Protection Regulation does not automatically end when the General Data Protection Regulation comes into effect.

[27] Cf. resolution of the Düsseldorfer Kreis of 24/25 November 2010, p. 2
[28] Also Marschall/Müller ZD 2016, 415, 416
[29] Hereafter referred to as 'certificate of appointment'
[30] Cf. section 5 of the appointment document

1.2.2 Question: *"Does an order placed before the entry into force of the General Data Protection Regulation automatically end when the General Data Protection Regulation comes into effect*?

In principle, the termination of the civil law contract is governed both by the consultancy agreement, which always forms the basis of the assignment, and by the statutory termination provisions of service law.
As a result, the provisions governing the termination of an employment relationship pursuant to Articles 620 ff. BGB (German Civil Code) apply. This is because, as already explained at the beginning of point 1.2, the exercise of the activity of the operational officer for data protection represents a paid business arrangement and thus a mixed contractual relationship consisting of a service contract and a mandate, whereby according to Article 675(1) BGB the provision for revocation of the mandate is not applicable since Article 671 BGB does not apply.
According to Article 620(1), (2) BGB (German Civil Code) the mandate ends either by expiration of time or by achievement of the contract purpose agreed in advance. However, the change in the legal basis for the designation of a data protection officer when the General Data Protection Regulation comes into effect does not constitute an intrinsic time limitation. This already results from the general principle of Article 620(1) BGB, according to which a continuing obligation ends at the end of the period for which it was entered into.[31] This therefore refers to a fixed term of the contract agreed in advance. A time limit does not exist if the legal basis for the appointment or designation of the data protection officer changes.
Nor can the achievement of the purpose of the contract be seen in the fact that the legal situation changes accordingly. In order to avoid repetitions, reference is made to what has been said in points 1.1.1 and 1.2.1. The business purpose of appointing the data protection officer is not achieved by the entry into force of the General Data Protection Regulation. A mental distinction must be made between the attainment of the purpose and the removal of the purpose. In the case of the former, the objective of the mandate, which was defined in advance, has been achieved; in the case of the removal, the objective has not been achieved, but it should no longer to be achieved due to a particular change in circumstances.
The purpose of the assignment according to Article 1 of the sample consultancy agreement provided[32] is the performance of the function of operational data protection officer in the sense of Article 4 f (1) BDSG. This will remain in place even after the entry into force of the General Data Protection Regulation. The same purpose would also exist without a separate contractual provision, since the purpose of the appointment of an external data protection officer can be readily inferred from Article 4 f (1) BDSG. Again, the purpose of the appointment would not be achieved by the entry into force of the General Data Protection Regulation.

An automatic legal termination of the appointment is neither governed by the Federal Data Protection Act nor the General Data Protection Regulation nor Article 620 ff. BGB (German Civil Code) so that, in the opinion of the persons responsible for this expert opinion, a legal

[31] Hesse in MünchKomm BGB, 6th edition 2012, Article 620 marginal 1
[32] Hereinafter referred to as 'the consultancy agreement'

basis for the appointment made before the General Data Protection Regulation does not automatically end with the entry into force of the General Data Protection Regulation.

A removal of the business basis in accordance with Article 313 BGB (German Civil Code) may be considered if the requirement to designate a data protection officer ceases with the entry into force of the General Data Protection Regulation. In this case, the premise under which the consultancy agreement was concluded changes fundamentally. However, the legal consequence of this is not the automatic termination of the consultancy agreement.

The appointment of an external data protection officer before the entry into force of the General Data Protection Regulation does not automatically end when the General Data Protection Regulation comes into effect.

1.2.3 **Question:** *"Does the entry into force of the General Data Protection Regulation constitute a reason for dismissal*

1.2.3.1 Question: *... if there is no longer a requirement under the GDPR to designate a DPO*"?

This question has already been answered in the context of the comments in point 1.1.4.1. As already stated in this expert opinion, the appointment or designation of the data protection officer does not distinguish between internal and external data protection officers, so that the above remarks also apply to the external data protection officer. As already mentioned, the appointment or designation must be logically separated from the assignment of the external data protection officer.

According to the authors of this expert opinion, a reason for the dismissal of a data protection officer can only be considered if the legal requirements for the mandatory appointment of a data protection officer have changed and a duty to appoint no longer exists. In the opinion of the authors of this expert opinion, however, this is not the case with regard to the Adaptation Act (AnpassungsG) and the BDSG-new.

As a result, the entry into force of the General Data Protection Regulation does not constitute a reason for dismissing an external data protection officer if the General Data Protection Regulation no longer requires the appointment of a data protection officer.

1.2.3.2 Question: *"... even if there is a requirement to designate a DPO under the GDPR?*"

This question was also answered in the comments in points 1.1.4.1 and 1.1.4.2. In the opinion of the authors of this expert opinion, there is no reason for the revocation of the external data protection officer as a result of the entry into force of the General Data Protection Regulation, even if there is a requirement to designate a DPO.

The question must therefore be answered in the same way as question 1.2.3.1, provided, however, that - even if the BDSG-new should not come into effect - the entry into force of the General

Data Protection Regulation would not give rise to a revocation of the external data protection officer if a requirement to designate a DPO also exists under the provisions of the General Data Protection Regulation.

1.2.4 **Question:** *"Does the entry into force of the General Data Protection Regulation constitute an extraordinary or ordinary reason to terminate the contract*

1.2.4.1 Question: *... if there is no longer a requirement under the GDPR to designate a DPO?*"?

It has already been established in the preceding compilation that the entry into force of the General Data Protection Regulation cannot lead to an automatic termination of the appointment of the external data protection officer due to the provision in Article 620 BGB. The same applies to the status relationship of the appointment or designation. This also does not end automatically or due to a legal regulation. Rather, it always requires revocation as a unilateral act in accordance with Article 38(3) sentence 2 General Data Protection Regulation.

Article 621 BGB (German Civil Code) applies to a termination of the consultancy agreement, unless otherwise contractually agreed and the regulation is thereby waived. The consultancy agreement submitted regulates a term, so that the termination provision of Article 621 BGB does not apply. In the present analysis, termination is based on the contractual agreements. Article 8 of the consultancy agreement stipulates a contract term of two years, including an automatic extension of two years, unless terminated in advance. A regular termination is therefore only possible within this framework.

An existing right of termination due to the entry into force of the General Data Protection Regulation could at most be justified by the fact that there is a case in which there would no longer be an obligation to appoint or to designate a DPO due to the then new legal situation. Due to the BDSG-new that has now been passed, however, this is hardly conceivable, as has already been stated several times.

As a result, the entry into force of the General Data Protection Regulation does not constitute an extraordinary or ordinary reason to terminate the consultancy agreement of the external data protection officer if the General Data Protection Regulation no longer imposes an obligation to designate a DPO.

1.2.4.2 Question: *"... even if there is a requirement under the GDPR to designate a DPO?*"

This question has already been answered in the comments in point 1.2.4.1. In order to avoid repetition, reference is made to the above remarks.

If at all, it would be conceivable that the entry into force of the General Data Protection Regulation would constitute a reason for the termination of the consultancy agreement with the external data protection officer if, on the basis of the provisions of the General Data Protection Regulation in conjunction with the BDSG-new, a previously existing obligation to

appoint or designate a DPO were no longer to apply. However, as has already been mentioned several times, this cannot be assumed.

For the aforementioned reason, the entry into force of the General Data Protection Regulation does not constitute an extraordinary or ordinary reason for the termination of the consultancy agreement of the external data protection officer even if there is a requirement to designate a DPO under the General Data Protection Regulation.

1.3 Protection of the designated data protection officer in the GDPR

Question: *'Does the provision in the second sentence of Article 38(3) of the General Data Protection Regulation constitute protection against dismissal for the appointed salaried data protection officer? (Also in connection with last sentence of recital 97.)*"

According to its wording, the General Data Protection Regulation contains significantly less protection of the salaried data protection officer against sanctions by the employer than the provisions of the currently applicable Federal Data Protection Act or the BDSG-new.

Article 38(3) sentence 2 GDPR provides that the data protection officer may not be removed or penalised by the controller or the processor "due to the performance of his duties".

In the recitals (ErwG 97) to the General Data Protection Regulation, the European legislator has in particular stated that data protection officers, whether or not they are employees of the controller, "may exercise their duties and tasks fully independently".

The General Data Protection Regulation therefore does not provide protection against dismissal for the data protection officer by its actual wording.[33] The text of the General Data Protection Regulation merely provides for protection against dismissal and a general prohibition of discrimination. As already mentioned, with regard to the legal classification of the data protection officer, a distinction must be made between his status (designation/revocation) and the basic relationship of his activity (employment relationship/agency contract). However, in large parts of the literature the view is expressed that a data protection officer who has been dismissed (under labour law) and who has not yet been recalled can hardly fulfil his duties as data protection officer in a meaningful way.[34] For this reason, the legal literature takes the view that the above-mentioned wording of Article 38(3) GDPR is to be understood in such a way that not only dismissal and other discrimination, but also termination of the employment relationship of the designated data protection officer "due to the fulfilment of his duties" should not be permissible.[35]

[33] Ehmann/Selmayr, loc. cit., Article 37, marginal 14; Ettig/Bausewein in Wybitul, Handbuch EU-DS (Handbook EU-GDPR), Article 38 marginal 21
[34] Bergt in Kühling/Buchner, Datenschutz-Grundverordnung Kommentar (General Data Protection Regulation Commentary) 2017, Article 38 marginal 32; similarly probably to the Bussche in Plath, BDSG GDPR, Article 38 marginal 10 f
[35] Bergt in Kühling/Buchner, General Data Protection Regulation Commentary, 2017, Article 38 marginal 33

As already mentioned, the BDSG-new contains provisions on protection against dismissal of the designated data protection officer. In general, it should be noted that the appointed data protection officers, who are also employees of the controller, can only be dismissed if evidence exists which entitles the public body (Article 6 BDSG-new) or the controller (Article 38(2) BDSG-new) to pronounce dismissal for good cause without observing a period of notice. This special protection against dismissal of the data protection officer only applies to non-public bodies if the designation of a data protection officer is mandatory (Article 38(2) BDSG-new). The provisions of the BDSG-new are thus very closely aligned with the provisions of the currently applicable Federal Data Protection Act. The termination of the employment relationship within one year is inadmissible even after the end of the activity as data protection officer, unless the public body or the controller is entitled to terminate the employment relationship for an important reason without observing a period of notice (so-called follow-on termination protection).[36]

As a result, this means that it follows from the General Data Protection Regulation and in particular also from Article 38(3) GDPR as well as recital (ErwG) 97 that data protection officers enjoy at most limited protection against dismissal, which according to the clear wording of Article 38(3) GDPR is limited in this respect to the fact that the data protection officer may not be dismissed "due to the performance of his duties". Other reasons for termination, such as operational reasons for termination or reasons for termination, which are based on the person of the data protection officer, are not covered by the protection against dismissal of the General Data Protection Regulation.

On closer examination, the protection of the data protection officer against dismissal by the employer as standardised in the General Data Protection Regulation thus proves to be relatively weak. It is doubtful whether a data protection officer who is only protected by the provision in Article 38(3) GDPR is able to carry out his activities with the independence required by the General Data Protection Regulation itself. In this respect, with reference to recital (ErwG) 97, an attempt could be made to extend the protection against dismissal under Article 38(3) GDPR beyond its mere wording. Such a "further development" of protection against dismissal on the basis of the meaning and purpose of the provisions of the General Data Protection Regulation would not be in too blatant a contradiction to the general legal interpretation regulations either, because in European Union law in particular so-called teleological interpretation, i.e. interpretation according to the meaning and purpose of a legal regulation, is of particular importance. In some cases, teleological interpretation within the framework of European law is given "supreme weight".[37] Starting from interpretation based on the meaning and purpose of a regulation, the European Court of Justice (ECJ) has often also resorted to the so-called principle of effectiveness (effet utile). In doing so, it has regularly preferred the interpretation that promises the greatest possible practical effectiveness of the European rules.[38] However, it must be clearly pointed out that any interpretation of the General Data Protection Regulation must not exceed its limits in the provisions on the legal

[36] Bergt, loc. cit.
[37] Albrecht/Jotzo, Das neue Datenschutzrecht der EU (The new EU data protection legislation), Part 1, marginal 30
[38] Albrecht/Jotzo, loc. cit., part 1 marginal 31

competence of the Union and the Member States. The power to regulate substantive labour law lies with the individual member states, so that in the end it will depend on national regulations such as the BDSG-new.[39]

The question must therefore be answered as follows:

It can be stated with good arguments under European law that Article 38(3) of the GDPR goes beyond its mere wording and provides for extensive normalised protection against dismissal by the data protection officer. This is in line, in particular, with the statements of the European legislator in recital (ErwG) 97. The question, however, is what scope this "extended" protection against dismissal should have. There is a lack of concrete guidance and it is not clear from the recitals or the rules of the General Data Protection Regulation itself. It therefore remains, as a (safe) assessment, that the General Data Protection Regulation provides weak protection against dismissal for data protection officers in terms of its wording, but that this protection, however, is concretised and extended by the provisions of the BDSG-new – a fact which is certainly to be welcomed due to the associated legal certainty. According to the authors of this expert opinion, the fact that the provisions of the BDSG-new on protection against dismissal of the data protection officer are likely to be in conformity with European law also results in particular from the recitals to the General Data Protection Regulation and the fact that an effective activity of the data protection officer is only likely to be possible if there are precisely manageable protection provisions.

1.3.0 Preliminary remark to 1.3.1: Fundamentals of civil liability of the data protection officer

In order to answer the question of civil liability, the basis for such liability must first be presented in order to provide a better understanding. These aspects then also have a mirror image effect on the possibilities for limiting liability, which is the subject of question 1.3.4.

Against the background of the current situation, the data protection officer's liability due to omission needs to be examined more closely. This is presented under point 1.3.0.1, taking into account the overall circumstances arising from the General Data Protection Regulation (see point 1.3.0.1.1).

The common conditions of civil liability outside the brackets are set out below, as they apply equally to the establishment and fulfilment of the data protection officer's liability - whether internal or external. The individual prerequisites lead to overall liability if they are met.

[39] Lepperhoff/Müthlein, Leitfaden zur Datenschutz-Grundverordnung (Guide to the General Data Protection Regulation), 2017, p. 85

The prerequisite for liability is the existence of a culpable breach of duty through either active action or omission, which must have resulted in causal damage.

- **Breach of duty**

The prerequisite for the liability of the external, designated data protection officer is the breach of a duty to perform. These will therefore be dealt with in greater detail in the following. For without an obligation to perform, no breach of duty will exist and without a breach of duty no liability. A breach of duty can also consist in a failure to act. However, this is only the case if the data protection officer is also obliged to act, but no action is taken. For example, in the case of non-prevention of a data protection violation within the framework of monitoring, if there is a duty to act. The General Data Protection Regulation is based on a system of monitoring and action in terms of its legal structure and system. The concept of monitoring must be integrated into this system as an overall consideration. For an isolated view of the term overlooks fundamental points that result in a different assessment.

The possible breaches of duty by the data protection officer are listed below:

- **Breach of duty in the form of: Breach of a contractual obligation**

  If the data protection officer violates his primary contractual obligations, e.g. by revealing secrets of the client company, a breach of duty can reasonably be assumed. This is clear in this respect and is dealt with in this expert opinion only briefly with regard to the relevance for criminal law (cf. excursus after question 2.2.1).

  A breach of a contractual obligation may also exist if a further obligation to act on the part of the data protection officer is agreed in the consultancy agreement, such as if he is also granted the right to issue instructions.

  A distinction must be made between contractual obligations and legal obligations of the data protection officer. Only the latter are the subject of this expert opinion.

- **Breach of duty in the form of: Breach of data protection by the data protection officer**

  The data protection officer can, like any other actor in a company, violate data protection regulations himself, for example by passing on personal data to a third party without the consent of the data subject.

- **Breach of duty in the form of: Infringement of a statutory duty pursuant to Article 39 GDPR (through active action)**

  According to Article 39(1) lit. a GDPR, the data protection officer is responsible for informing and advising the controller or the processor and the employees carrying out the processing operations with regard to their duties. Pursuant to Article 39(1) lit. c GDPR, he has the duty to provide advice in connection with the data protection impact assessment. In addition, Article 39(1) lit. d GDPR stipulates that he is also responsible for cooperation with the supervisory authority, and Article 39(1) lit. e GDPR stipulates that he is also the contact point for the supervisory authority in matters related to processing.

  If one of the aforementioned conditions is incorrectly applied, for example if the data protection officer provides the controller with incorrect information during consultations, a breach of duty can also reasonably be assumed.

- **Breach of duty in the form of: Non-prevention of a data protection violation in the company**

  A breach of duty can also exist if someone omits an action although he is obliged to do so. Failure to do so always presupposes a duty to act, be it - as explained above - from the contract or from the statutory tasks assigned to the data protection officer.

  For the data protection officer there is no obligation per se - of any kind - to prevent data protection breaches.

  According to Article 39(1) lit. b GDPR, the data protection officer, whether internal or external, is responsible for the following:

  > *"Monitoring compliance with this Regulation, other data protection legislation of the Union or the Member States, and the policies of the controller or processor for the protection of personal data, including the allocation of responsibilities, awareness-raising and training of staff involved in the processing operations and related verifications*."

  At first glance, this may result in a prevention duty. The concept of monitoring is not regulated in the GDPR itself,[40] but it is decisive for the question of whether and when a breach of duty on the part of the data protection officer has occurred.

[40] So also Marschall/Müller ZD 2016, 416, 418

Excursus on the old legal situation of the previously applicable Federal Data Protection Act:

Previously, Article 4 g (1) sentence 4 no. 1 BDSG of the Federal Data Protection Act (Bundesdatenschutzgesetz) also stipulated that the data protection officer was to monitor the proper use of the data processing programmes used to process personal data. According to the Federal Data Protection Act, monitoring the proper use of data processing programs is one of the focal points of the data protection officer's activities. Monitoring is an accompanying check which is intended to prevent unlawful processing of personal data at all.[41] The data protection officer is obliged to check the compatibility of the processing programs already introduced or only planned with the requirements of data protection and to report this to the controller. However, he is not obliged to explain how the corrections required in his view can be implemented in detail.[42] This means that monitoring within the meaning of the Federal Data Protection Act is limited to checking existing or planned processing programs for their compatibility with data protection law, but does not, however, make concrete changes to the existing or planned program or even propose them. According to the Federal Data Protection Act, the responsibility for data protection lies with the office responsible according to Articles 2, 3 (7) BDSG and thus in the non-public area of the management of the respective data processing company. This means that the task of the data protection officer for monitoring ends with a report to the management.

An interpretation of the General Data Protection Regulation on the basis of this understanding is naturally not possible. The General Data Protection Regulation is to be interpreted as a Union law ordinance in its own right and not from the perspective of a national predecessor law.[43] This applies even against the background that the Federal Data Protection Act was clearly the inspiration for the provisions in Article 37 to 39 GDPR.

Deviating from the provisions of the Federal Data Protection Act, the General Data Protection Regulation is based in its legal structure on a monitoring and action system. This means that the concept of monitoring may impose additional obligations on the DPO, which also require action by the DPO himself.

If an obligation to act arises from the word "monitoring", there may be a breach of duty if a necessary action is omitted. The question of the duty to monitor is dealt with in greater detail in point 1.3.0.1.3 below, whereby this cannot be viewed in isolation for the sake of overall understanding, but the organisation must first be described in point 1.3.0.1.1 and then included in a derivative form.

[41] Gola/Schomerus, BDSG, 12th edition 2015, Article 4g BDSG marginal 18
[42] Simitis, Federal Data Protection Act, 8th edition 2014, Article 4g marginal 46
[43] Roßnagel MMR 2015, 359

- **Culpability**

A culpable breach of duty is required for the establishment of liability. Basically, everyone is liable for intent and negligence if no statutory liability privileges are apparent.[44] This also applies to the external data protection officer, but not to the internal one, as will be explained in point 1.3.1. The culpability must exist in relation to the respective breach of duty.

Article 39(2) GDPR cannot be construed as a liability privilege. The provision is intended to regulate the manner in which the tasks are to be performed in accordance with Article 39(1) GDPR and stipulates that the data protection officer must take due account in the performance of his duties.[45] The statutory provisions of Articles 675, 611 ff. BGB (German Civil Code) which are relevant for the external data protection officer also provide no liability privileges. Other statutory liability privileges are not apparent.

Intent is the knowledge and wilfulness of the breach of duty. It is already sufficient for this purpose if the breach of duty is recognised and tacitly accepted. In the case of culpability due to a failure to act, this means that the duty to act is recognised but ignored.

Anyone who neglects the care required in traffic acts negligently, cf. Article 276(2) BGB. In contrast to criminal law, an objective rather than a subjective standard is applied.

The level of diligence to be exercised by the data protection officer will therefore depend on the level of diligence to be applied to him. As a rule, the yardstick used is the degree of prudence and diligence a prudent and conscientious member of the relevant public would have observed in the specific situation.[46] The objective yardstick will have to be determined on the basis of the requirements addressed by the General Data Protection Regulation in Article 37 (5) GDPR, namely the particular professional qualifications and expertise of the data protection officer. The corresponding mission statements of the data protection officer will also be included in the evaluation.[47]

To this end, the breach of duty must have been foreseeable for the data protection officer. The general foreseeability of an injurious outcome is sufficient here, the details of the specific course of events need not be foreseeable.[48]

It follows already at this point that the culpability criterion of "negligence", which is relevant in the following, cannot be regarded as a fixed term. It depends in particular on the level of objectified care that can be expected from a data protection officer. Therefore, in the present

[44] Grüneberg in Palandt, 76th edition 2016, Article 276 BGB marginal 1
[45] Paal in Paal/Pauly, Datenschutz-Grundverordnung (General Data Protection Regulation), 1st edition 2017, Article 39 GDPR marginal 2
[46] Grüneberg in Palandt, 76th edition 2016, Article 276 BGB marginal 17
[47] BvD, Das berufliche Leitbild des Datenschutzbeauftragten (The professional mission statement of the Data Protection Officer), 3rd edition 2016
[48] Grüneberg in Palandt, 76th edition 2016, Article 276 BGB marginal 20

case, the content of the service can have a liability limiting effect within the scope of fault.

➢ **Causal damage**

Not every damage, which has any cause in the breach of duty of the data protection officer, is to be regarded as causal in terms of liability law. In a first step, it must be established that the damage was caused precisely by the event obligating the claimant to pay damages.

In a second step, there must be an adequate causal damage scenario. This means that dutiful conduct can be regarded as an adequate, typically appropriate condition for damage. If the action does not cause the damage directly, but only indirectly due to the addition of further circumstances, a third, evaluative consideration will be added as a corrective to the liability. The damage must also be such that the breached obligation should protect against the actual damage. This step also requires an evaluative consideration, which - like the second step - must be carried out by a court in the event of a dispute and can only be determined on the basis of the situation and not as a whole.

- **Breach of the causal link**

  In concrete situations, there may be interruptions in the attribution of causality, for example in the event of an intentionally acting third party intervening, or if the damage would also have occurred if the data protection officer had acted lawfully.[49]

- **Contributory negligence**

  In the context of contributory negligence also, the claimant of the damages can be held responsible for the fact that the damage can also be attributed to him.[50] This can lead to a minimisation of the claim up to an exclusion of the liability of the data protection officer. The decisive factor is what obligations the claimant himself has. This will be discussed in more detail in point 1.3.3.

1.3.0.1 Liability of the data protection officer in the event of non-prevention of a breach of data protection within the company

In the following, the above-mentioned category of "non-prevention of a breach of data protection within the company" as a breach of duty by the data protection officer is examined in more detail.

[49] Cf. Oetker in MünchKomm BGB, 7th ed. 2016, Article 249 marginal 142
[50] Cf. Oetker in MünchKomm BGB, 7th ed. 2016, Article 254 marginal 3

In its legal structure and systematics, the General Data Protection Regulation assumes an independent monitoring and action system.[51] The concept of monitoring must be integrated into this system in an overall view. For an isolated view of the term overlooks fundamental points that lead to a different assessment. Any isolated view of the term "monitoring" overlooks fundamental aspects. The monitoring and action system of the General Data Protection Regulation must therefore be described in advance. Only together with this description can the duty of the data protection officer to monitor be systematically classified and assessed in terms of liability.

1.3.0.1.1 Monitoring and action system of the General Data Protection Regulation

The controller is the person held responsible. This results from Article 5(2) GDPR. The responsibility is clearly and explicitly assigned to this person. The General Data Protection Regulation imposes additional accountability obligations on him for compliance with this responsibility.[52] The controller is therefore placed at the centre of compliance with the provisions of the General Data Protection Regulation.

The monitoring and action system of the General Data Protection Regulation is governed by Articles 5, 12 and 24 of the GDPR. At the centre of this system are therefore the controller and the corresponding organs of the company.[53]

- **Article 5 GDPR**

  Article 5 GDPR regulates the principles of a legally compliant processing of personal data.[54] These principles are not merely the setting of programmatic objectives but binding requirements for data processing authorities.[55] The principles set out here in a rather abstract manner are defined in the further regulations, so that a violation of the more far-reaching provisions of Article 6 ff. GDPR must always also be regarded as a breach of Article 5 GDPR.[56] Article 5 GDPR must therefore be seen as the "general standard" of data protection.

  Controllers are held accountable for their compliance with the substantive legal requirements laid down in Article 5(1) GDPR, i.e. the principles of

  - Legality
  - Processing in good faith
  - Transparency[57]

[51] Cf. Heberlein in Ehmann/Selmayr, Datenschutz-Grundverordnung (General Data Protection Regulation), 2017, Article 37 marginal 1
[52] Cf. also Hamann BB 2017, 1090, 1091 f.
[53] So also Behling ZIP 2017, 697, 699 f.
[54] Cf. Schantz NJW 2016, 1841, 1843; Hamann BB 2017, 1090 f.
[55] Hamann BB 2017, 1090, 1091
[56] So also Herbst in Kühling/Buchner, Datenschutz-Grundverordnung (General Data Protection Regulation), Article 5(1)
[57] Herbst in Kühling/Buchner, Datenschutz-Grundverordnung (General Data Protection Regulation), Article 5 marginal 7

It follows from Article 5(2) GDPR that the controller is accountable for compliance with the principles for processing and that he must be able to prove compliance with the principles.[58] According to Article 4(7) GDPR, the controller is any data processing authority within the European Union in the non-public sector, i.e. normally a company.[59] Accountability means that the obligation to document data processing is the responsibility of the company itself and thus of the management entrusted with directing the business.[60]

The documentation obligation is intended to encourages the controller to comply with the lawfulness of the processing from the outset. Article 5(2) HS. 2 GDPR forces the controller to fulfil the specified obligations. The obligation to document thus serves to safeguard data protection.[61]

A breach of the provisions of Article 5(1) GDPR is already assumed if the responsible body - and thus the management – is unable to provide evidence of data processing in accordance with the General Data Protection Regulation.[62] A breach of the documentation obligation under Article 5(2) GDPR is sanctioned with a so-called "large fine" within the meaning of Article 83(5) GDPR. In this case, fines of up to €20 million or, in the case of a company, up to 4% of its total worldwide annual turnover of the previous financial year are possible, depending on which of the amounts is higher.

Two things can be inferred from this: On the one hand, the location of the sanction lies with the management of the company itself and not with the data protection officer. On the other hand, the fact that a "large fine" is imposed for a breach of the documentation obligation indicates the legislative intention for the management itself to meet the relevant obligations under the GDPR. It is responsible for organising the company in compliance with data protection laws.

- **Article 24 GDPR**

Article 24(1) GDPR regulates the obligation to ensure that processing is carried out in compliance with data protection regulations and to be able to provide evidence that it is carried out in compliance with data protection regulations.[63] According to Article 24(1) sentence 2 GDPR, the organisational measures required for this purpose must be reviewed and updated as necessary.[64]

The regulation explicitly addresses the controller. This expresses the fact that the controller adopts a central position in terms of data protection responsibility.

[58] Sachs/Kranig/Gierschmann, Datenschutz-Compliance nach der DS-GVO (Data protection compliance in accordance with GDPR), p. 24; method CR 2016, 714, 716

[59] Ernst in Paal/Pauly Datenschutz-Grundverordnung (General Data Protection Regulation), 1st ed. 2017, Article 4 marginal 55

[60] Herbst in Kühling/Buchner, Datenschutz-Grundverordnung (General Data Protection Regulation), Article 5 marginal 77 ff.

[61] In conclusion also Wybitul CCZ 2016, 194, 197

[62] Cf. Sachs/Kranig/Gierschmann, Datenschutz-Compliance nach der DS-GVO (Data protection compliance in accordance with the GDPR), p. 110

[63] Piltz K&R 2016, 709, 710

[64] Sachs/Kranig/Gierschmann, Datenschutz-Compliance nach der DS-GVO (Data protection compliance in accordance with the GDPR), p. 24

- **Article 12 GDPR**

  Article 12 GDPR, in conjunction with Article 13 to 23 GDPR, regulates the duties to provide information to data subjects affected by data collection as well as the modalities for exercising the rights of data subjects.[65] It thus regulates the essential implementation requirements for the company, to which Articles 5 and 24 GDPR refer. Article 12 GDPR describes which measures are to be taken, in particular which information is to be provided. The standard stipulates that appropriate measures are taken by the controller (paragraph 1), that the controller facilitates the exercise of the rights of the data subjects (paragraph 2) and that the controller provides the data subjects with information on the measures taken (paragraph 3).

  A breach of the obligations under Article 12 GDPR is sanctioned with a "large fine" within the meaning of Article 83(5) GDPR. From this it can be deduced that the obligations within the meaning of Article 12 GDPR apply to the controller within the meaning of Article 4(7) GDPR. The amount of the fine also reflects the intention of the legislator to hold the company and the management acting on its behalf accountable and to require them to take appropriate measures themselves.

- **Data protection impact assessment**

  Article 35(1) GDPR stipulates that the controller must first carry out an assessment of the consequences of the planned processing operations for the protection of personal data if, due to the nature, scope, circumstances and purposes of the processing, a form of processing is likely to entail a high risk for the rights and freedoms of natural persons.[66] According to Article 35(2) GDPR, the controller must seek the advice of the data protection officer when carrying out such an assessment.

  The data protection impact assessment pursuant to Article 35 GDPR makes clear the relationship between the data protection officer and the controller in three respects.

  Although the legal situation which applied under the Federal Data Protection Act (BDSG) cannot be used to interpret the General Data Protection Regulation, the presentation nevertheless makes clear the different way of thinking under the General Data Protection Regulation. Under Article 4(1) sentence 1 BDSG in conjunction with 4 d (6) BDSG, the prior checking, which is now regulated in Article 35 GDPR, was the sole task of the data protection officer. This supplemented his duty to monitor and advise.[67] In the successor instrument to the General Data Protection Regulation, Article 35(1) GDPR, this original task is assigned solely to the controller.[68] In relation to the Federal Data Protection Act, therefore, it can be seen that a separate prior check by the data protection officer is no longer provided for.

[65] Schantz NJW 2016, 1841, 1845
[66] Kühlung/Martini EuZW 2016, 448, 452
[67] Simitis, (Bundesdatenschutzgesetz (Federal Data Protection Act), 8th ed. 2014, Article 4g, marginal 81

[68] Cf. Wise ZD 2016, 315, 318

The DPO does not play an independent role in complying with the requirements of Article 35 GDPR.[69]

Here, too, it can be seen that the General Data Protection Regulation assigns a secondary role to the data protection officer, a secondary position whose advice is sought by the controller at the centre of data protection. In principle, the data protection impact assessment could also be included in the concept of "monitoring" alone. But then it would not have been necessary to clarify that the data protection officer should only be consulted.

- **No enforcement powers**

Within a corporate structure, the executive bodies of the company are basically authorised to carry out actions and organise their company. If this possibility is also to be granted to an employee or a third party outside the corporate structure, it requires a conferral of authority, either by the company or its executive bodies or by law, in order to act.

The data protection officer differs from the company and its executive bodies in that he has no entrepreneurial or organisational powers to act within the context of carrying out his data protection tasks. The General Data Protection Regulation does not give him the power either to act accordingly. The GDPR leaves the formulation of civil law to the regulations of the member states.

This once again draws attention to the secondary role of the data protection officer. Although his task is to check compliance with data protection law, he does not, however, receive any intrinsic powers to act in order to be able to put an end to possible infringements. He reports possible breaches to the controller.

- **Target of sanctions**

Ultimately, it can also be seen from an overall viewpoint that the data protection officer is not mentioned in the provisions on sanctions in Article 83 GDPR. The controller and the processor are explicitly named. This also shows that the data protection officer plays a secondary role in data protection law and is not the focus of sanctions for infringements of duty.

- **Summary**

The data protection officer is not mentioned in Articles 5, 24 and 12 GDPR, so that the obligations laid down therein cannot affect him intrinsically. He is not the central body for data protection within the meaning of the General Data Protection Regulation. According to the above explanations, this is undoubtedly the controller according to Article 4(7)

[69] So also Jaspers/Reif RDV 2016, 61, 66

GDPR.[70] This also means that the responsibility - seen in the overall context - cannot simply be passed on.

A similar conclusion can also be assumed with regard to the provisions on sanctions in Articles 82, 83 GDPR. These do not include the data protection officer. Only controllers and processors are expressly named as liable parties. However, a DPO is neither of these. In this respect, the terms used represent a paradigm shift from the Federal Data Protection Act, which in Article 43 BDSG with refers to everyone - including the data protection officer with *"It's an offence to*". However, this can no longer apply due to the wording of the General Data Protection Regulation.

1.3.0.1.2 Legal status of the data protection officer

Pursuant to Article 38(1) GDPR, the data protection officer must be duly and promptly involved in all matters relating to the protection of personal data. This is a basic prerequisite for his effective performance. It is the duty of the controller and the processor to ensure that this is the case. Pursuant to Article 38(3) sentence 3 GDPR, the data protection officer has a direct right to report to the highest management level, which he informs pursuant to Article 39(1) lit. a GDPR.[71] At the same time, Article 38(4) GDPR stipulates that data subjects may consult the data protection officer. The same applies to the exercise of their data protection rights under the General Data Protection Regulation. This is likely to refer to the rights of data subjects under Articles 12 to 23 of the General Data Protection Regulation.[72]

It can therefore be seen that the Data Protection Officer is intended in particular to play an advisory and mediating role in the system of the General Data Protection Regulation. The controller and the processor are also subject to obligations under Article 38 GDPR. They are also the target of sanctions if the duties to "safeguard" are not observed. Pursuant to Article 83(4) GDPR, in the event of infringements, a so-called "small fine" will be imposed. In this case, fines of up to €10 million or, in the case of a company, up to 2% of its total annual worldwide turnover in the preceding financial year are possible, whichever is the higher. The data protection officer, on the other hand, is not targeted by any sanctions.

From the system of the General Data Protection Regulation (as described in point 1.3.0.1.1) and the legal position of the data protection officer, the following can be concluded from an overall viewpoint:

The data protection officer is not the "central body" of data protection within the meaning of the General Data Protection Regulation. He is not subject to the essential obligations of the General Data Protection Regulation. These exclusively affect the controller and thus the

[70] Behling ZIP 2017, 697, 699 also reaches the same result
[71] Klug ZD 2016, 315, 318; Hamann BB 2017, 1090, 1096
[72] Klug loc. cit.

company itself. The controller bears the overall obligation to regulate the tasks and measures imposed by the General Data Protection Regulation. The data protection officer only plays an “outsider” role in the overall view of the monitoring and action system. Against this background, the term "monitoring" will have to be interpreted (see point 1.3.0.1.3 below).

1.3.0.1.3 "Monitoring"

Pursuant to Article 39(1) lit. a GDPR, the data protection officer informs and advises the controller and the employees with regard to their duties.[73] This task includes informing the controller about processes relevant to data protection by the data protection officer reporting to him.[74]

Article 39(1) lit. b GDPR supplements the tasks of the data protection officer regulated in Article 39(1) lit. a GDPR with a control function, which also includes internal "strategies" for the protection of personal data.[75] The interpretation of the term has so far hardly been discussed in the literature. The term "monitoring" points to an ambivalent, but rather passive term. The same impression results from the wording of the English ("monitor") and French ("contrôler") texts of the Regulation, which, to judge by their meaning, imply a perhaps passive surveillance.[76] According to the meaning of the word, "monitoring" can also be understood as "observation" and "logging". It can be inferred from recital 97 that "monitoring" is intended to be a supportive task for the controller or the processor.[77] However, it cannot be inferred from this that active control is necessary.[78]

Nevertheless, the interpretation of each particular term does not seem to be constructive, but the term should be seen as a uniform "monitoring of compliance with this Regulation". In the overall context of the explicitly regulated organisational obligations outlined above, it becomes clear that "monitoring compliance with this Regulation" can only be understood as a review of the organisational structure under data protection law, which the responsible party itself must establish in accordance with the provisions in Articles 5, 24, 12 GDPR.[79]

The data protection officer has neither the task nor the authority to establish a second data protection structure in order to prevent breaches of data protection regulations.[80] While actions are prescribed for the controller ("takes measures", "must prove", "provides information"), the data protection officer has not been given any such duties to act or even opportunities to act.

[73] Cf. Klug loc. cit., 318
[74] Cf. Thode CR 2016, 714, 718; Klug loc. cit.
[75] Klug loc. cit.
[76] A.A. Marschall/Müller ZD 2016, 415, 418
[77] So also Heberlein in Ehmann/Selmayr, Datenschutz-Grundverordnung (General Data Protection Regulation), 2017, Article 39 marginal 10
[78] A.A. Marschall/Müller ZD 2016, 415, 418
[79] So also Ettig/Bausewein in Wybitul, Handbuch EU-Datenschutz-Grundverordnung (Handbook EU General Data Protection Regulation, Article 39 marginal 16
[80] See also Behling ZIP 2017, 697, 699 f

The originally planned task of "safeguarding" the documentation was dropped during the tripartite negotiations.[81]

Monitoring in the conventional sense would also require the possibility of an intervention in the process in order to eliminate the error in terms data protection law if necessary. However, this would require the data protection officer to have the corresponding authority to issue instructions.[82] This same cannot be inferred from the General Data Protection Regulation. Although monitoring pursuant to Article 39(1) lit. b GDPR includes the allocation of responsibilities to employees,[83] in the view of this party, no further authority to issue instructions can be derived from this. According to the wording, the allocation also serves only the purpose of the monitoring itself, not the elimination of any data protection-infringing states that may be uncovered.

Article 38(3) GDPR assigns the data protection officer the task of reporting to the highest management level. Additional duties to act or authority to issue instructions are not provided for.[84]
If the external data protection officer has authority to issue instructions in the consultancy agreement or - in the case of an internal data protection officer - in a supplementary agreement, this has a corresponding effect on his liability.[85] This was not done in the consultancy agreement provided, so that this is not elaborated any further in the present draft. Neither the General Data Protection Regulation nor the BDSG-new give rise to any intrinsic authority to issue instructions. This is also in line with the view of the evaluators of this expert opinion that, according to recital 97, monitoring by the data protection officer is a supporting measure for those actually responsible, namely for the company itself and for the processor.

There is strong doubt, as stated above, that the data protection officer has the role of preventing any breach of data protection within the company. This also results from the protective purpose of the standard. This is because it is not designed in such a way that every breach of data protection should be prevented. Rather, the standard is designed so that information is obtained about breaches of data protection, and that the data protection officer brings these the attention of the controller who then rectifies them. Monitoring therefore means monitoring the data protection organisation of the controller.

In summary, the following applies:

In principle, the General Data Protection Regulation stipulates that the data protection officer's duty to review and monitor the existing organisation of data protection must be such that its compatibility with data protection law and internal guidelines can be checked.

[81] Cf. Jaspers/Reif RDV 2016, 61, 65
[82] Marschall/Müller ZD 2016, 415, 418
[83] Paal in Paal/Pauly Datenschutz-Grundverordnung (General Data Protection Regulation), 1st ed. 2017, Article 39 marginal 6
[84] Jaspers/Reif RDV 2016, 61, 66; also Ettig/Brausewein in Wybitul, Handbuch EU-Datenschutz-Grundverordnung (Handbook EU General Data Protection Regulation, 1st edition 2017, Article 39
marginal 17

[85] Jaspers/Reif loc. cit.

The consequence of this is, unless otherwise stipulated in the contract, that the data protection officer is obliged to report a data protection infringement at the highest management level. The General Data Protection Regulation does not provide for a more far-reaching power of the data protection officer to issue instructions in order to remedy the identified breach himself, which is why the data protection officer, in the context of monitoring, has an obligation to inform the controller of a data protection breach of which he becomes aware, but not an obligation to remedy the data protection breach himself.

This is in line with the monitoring and action system of the General Data Protection Regulation. The controller is obliged to act under data protection law, as follows from Articles 5, 24, 12 GDPR. In the context of his duty of review, the data protection officer only has a supporting function which, in the opinion of the authors of this expert opinion, does not entail any duties to act beyond reporting to the management.

1.3.0.2 Result

In the opinion of the editors of this expert opinion, the data protection officer is not liable for any non-prevention of data protection infringements in the company. He adopts an "observer" role and reports data protection infringements to the controller. He does not have the task of preventing breaches of data protection and therefore has no duty to act, which would be necessary for any liability claims arising from omission.

1.3.1 Question: *"Under what circumstances can the employed data protection officer held liable?*"

It has already been explained in the context of the above remarks that the data protection officer - regardless of whether he is an external or an internal data protection officer - can be held liable for culpable breaches of duty in accordance with the relevant civil law regulations and standards. The view expressed from time to time that the data protection officer is not liable for breaches of duty has not, in the opinion of the authors of this expert opinion, been related to questions of labour law or general civil law.[86] For it is true that the person primarily responsible for compliance with the provisions of the General Data Protection Regulation and the so-called compliance regulations is the controller. However, this does not mean that general liability principles of civil and labour law would not apply to the data protection officer. Rather, it can be assumed that the General Data Protection Regulation does not create any additional civil or labour liability standards. At the same time, however, it does not eliminate liability principles under general civil and labour law. European legislators are not even

86 Guidelines on Data Protection Officers of Article 29 Data Protection Working Party dd. 13.12.2016, p. 4

empowered to make such statutory provisions. For it is primarily up to the national legislator to amend and define the regulations of labour law.[87]

According to this, the interim result is that an employed data protection officer is in principle liable under the same conditions as any other employee.

In the context of a long-term development of case law, the Federal Labour Court last defined in 2010 the principles of an employee's liability vis-à-vis the employer in the event of a culpable (i.e. at least slightly negligent) breach of legal obligations. In this context, the Federal Labour Court first of all worked out that an employment relationship constitutes a special civil-law obligation in which, due to the special personal ties between the contracting parties, a large number of ancillary obligations as well as duties to cease and desist and duties to act regularly arise. In addition, there are general duties of care, custody, welfare, information and notification which serve to promote the performance of the respective main duties of the parties to the employment contract, i.e. the employee and the employer, to maintain the performance capabilities and to secure the success of performance.[88]

According to the case-law of the Federal Labour Court cited above, an employee is liable to an employer for a breach of duty and culpable damage caused to the employer in accordance with the principles of the so-called operationally induced activity:

If the employee infringes legal interests of the employer within the scope of an operationally induced activity and thereby causes damage to the employer, an alleviation of liability may be considered. The employee's actions are prompted by the company if, from an objective point of view, they were in the interests of the company from the point of view of the injuring party, if his actions were not untypical in the light of customary commercial practice and if they did not constitute an excess.[89] Activities which were assigned to him under an employment contract or which the employee carries out for the company in the interests of the employer are considered to be prompted by the company. Action does not have to be part of the employee's actual area of responsibility; it is sufficient if he acts in the employer's best interests.[90]

The operational character of the activity is not lost through the employee's grossly negligent or even intentional breach of his duties during the performance of the activity, even if such conduct is in principle not in the employer's interest.[91]

Ultimately, this means that an employee's alleviation of liability, which is still to be specified below, can always be considered in the event of damage to the employer's legal assets if the damaging action took place within the context of job performance. A simple case in this

[87] Jaspers/Reif, RDV 2016, 61, 64
[88] BAG, jurisdiction dd. 28.10.2010 - 8 AZR 418/09
[89] BAG, jurisdiction dd. 22.04.2004 - 8 AZR 159/03
[90] BAG, jurisdiction dd. 14.03.1974 - 2 AZR 155/73
[91] BAG, jurisdiction dd. 28.10.2010 - 8 AZR 418/09

context would be, for example, that of the driver who damages another vehicle while manoeuvring in the depot. A case of so-called excess, i.e. a case in which no operationally induced activity could be assumed, would be that of the employee who, within the context of a dispute with colleagues, damages legal interests, such as furnishings or machines, of the employer.

As a general rule, the term 'operationally induced activity' is to be understood quite broadly.

Insofar as a so-called operationally induced activity exists, the principles developed by the Federal Labour Court on limited employee liability apply. According to this, an employee is in principle fully liable if he intentionally causes damage to the employer. In the case of only minor or very minor negligence, the employee is generally not held liable. In the case of moderate negligence, the damage is usually shared between the employer and the employee. In the case of gross negligence, the employee generally has to bear the entire damages, but alleviation of liability, depending on a case-by-case, may come into question.[92]

It is naturally difficult in individual cases to distinguish between the different degrees of negligence. The deliberate causation of damage, on the other hand, is quite easy to determine on a case-by-case basis. On the other hand, it is often difficult to assess whether there is a case of minor negligence or moderate negligence.

The Federal Labour Court itself has therefore determined that both the concept of culpability and the individual types of culpability (minor, simple, moderate and gross negligence) are legal concepts which are subject to assessment by the judge. The Federal Labour Court has therefore pointed out as a corrective for this legal uncertainty that even in the case of gross negligence, circumstances may arise which justify a limitation of liability. Here, for example, the Federal Labour Court referred to the amount of the employee's pay. An employee who is paid only a low wage cannot, in principle, be held liable in full even for damage caused by gross negligence.

These principles of employee liability, developed and consistently applied by the German labour court, also apply to culpable breaches of duty by the internal data protection officer and his liability towards his employer. However, even after the General Data Protection Regulation enters into force, it must be borne in mind that the data protection officer, due to the operational risk to be borne by the employer and the considerable contributory negligence of the company management (Article 254 BGB) – for example, due to inadequate

[92] BAG, loc. cit. (Fn 91)
[93] BAG, loc. cit. (Fn 91)

equipment of the data protection officer - should not normally be expected to accept full liability.[94]

Nevertheless, the internal data protection officer is also held liable for the fulfilment of the tasks and duties assigned to him through his employment contract as data protection officer within the meaning of the General Data Protection Regulation.

The General Data Protection Regulation governs a large number of the data protection officer's tasks and is not fully transparent and unambiguous in every respect.[95] Wording that is sometimes misleading is partly to the detriment of the legal certainty of the companies and ultimately, due to a certain legal uncertainty, also to the detriment of the data protection officers themselves.[96] However, it is in principle up to the claimant to present and prove the evidence that is intended to support his claim. This relative uncertainty about the tasks and obligations of the data protection officer, which stems from the General Data Protection Regulation, is reinforced by the consequences of a culpable breach of obligations on the part of the internal data protection officer, which are themselves difficult to foresee in practice.

Due to the uncertainties outlined above, it may be advisable in practice to define precisely the individual tasks and obligations of the DPO in the company in an intrinsic employment contract for an employee recruited as DPO or in the context of an agreement on the assumption of the position of DPO (in the case of a subsequent appointment as DPO). This would clarify for both the employee and the employer the exact responsibilities of the DPO in the company and also any breaches of obligations. An individual contractual regulation which is in line with the General Data Protection Regulation and which specifies the tasks and obligations of the data protection officer mentioned therein, should not be objectionable with regard to the liability of the internal data protection officer from the point of view of labour law.

Not included in the liability privileges of limited employee liability are any claims for damages which a data subject himself could hold against a data protection officer. Since the data subject himself as a rule has no contractual relationship with the data protection officer, the data subject's claims against the data protection officer may only arise from the point of view of a contract with protective effect in favour of third parties or from tort law in accordance with Article 823 ff. BGB (German Civil Code).

For example, a contract with a protective effect in favour of third parties could be seen in the agreement between the internal data protection officer and his employer under which the employee takes over the duties of data protection officer. An example of this could be the employment contract of a person originally employed as data protection officer or of a

[94] Gola/Brink in Boecken/Düwell/Diller/Hanau, Gesamtes Arbeitsrecht (Complete labour law), 1st edition 2016, Article 4 g BDSG, marginal 10
[95] Marschall/Müller ZD 2016, 415, 420
[96] Marschall/Müller, loc. cit.

supplementary agreement to the employment contract concerning the duties of the data protection officer.

A contract with protective effect in favour of a third party is a legal institution in which the two parties to a contract extend the protection of the contract to an uninvolved third party (e.g. one or an indefinite number of data subjects). Such a contract is characterised by the fact that the claim to the main services of the employment contract is solely due to the two contracting parties, but the third party is included in the contractual duties of care and custody in such a way that he can assert contractual claims for damages in the event of their infringement. The inclusion of a third party in the protective effect of a contract presupposes that the sense and purpose of the contract and the recognisable effects of the contractual services on the third party require its inclusion, taking account of good faith, and that a contracting party, recognisably for the other contracting party, can reasonably expect that the care and attention owed to it will also be extended to the third party to the same extent.[97]

So far, no legal view has been taken that the employment contract between an internal data protection officer and the controller or any other labour agreement between an internal data protection officer and his employer can in fact be considered as an agreement to protect an unpredictable number of data subjects. It cannot be assumed that the parties to such an agreement intend to extend the protection of the contract to data subjects, nor can it be assumed that this is in line with the provisions of the General Data Protection Regulation. Neither the General Data Protection Regulation nor the draft of the planned Adaptation Act provide for any direct liability or any further liability on the part of the data protection officer.

Although the data protection officer will continue to be referred to as the "lawyer of the data subjects" in future (Article 38(4) and (5) GDPR),[98] this is, however, hardly to be understood as meaning that the data subjects in their entirety should be included in the scope of protection of a contractual agreement between the data protection officer and the controller.

It is therefore conceivable that only a claim under so-called tort law pursuant to Article 823 ff. BGB (German Civil Code) remains. In this context, however, it should be noted that the damages incurred must be caused by the data protection officer's breach of duty. Since the General Data Protection Regulation has no means by which the data protection officer could effectively enforce his suggestions or proposals, the causal link between the failure to monitor or otherwise carry out his duties is likely to be missing in most cases.

It should also be pointed out that, pursuant to Article 24 GDPR, the processing of data in accordance with the provisions of the General Data Protection Regulation is the responsibility

[97] LAG Hessen, jurisdiction dd. 29.1.2015 - 5 Sa 922/14
[98] Jaspers/Reif RDV 2016, 61, 65; Lepperhoff/Müthlein, loc. cit. p. 86

of the controller. According to the concept of the General Data Protection Regulation, the data protection officer assumes a function within the framework of compliance.[99] The question of liability by omission in general will still have to be dealt with within the framework of the answer to question 1.3.3.

The internal data protection officer is liable for culpable breaches of duty in the same way as other employees. Due to the operational activity carried out by him, he benefits from an employee liability privilege.

1.3.2 Question: *"Under what conditions can the external (service contract) data protection officer appointed be held liable*?

The external designated data protection officer shall be liable in accordance with the relevant civil law regulations. It requires - as described in detail above under point 1.3.1 - a culpable breach of a contractual or statutory obligation to perform. However, he is not liable like a compliance officer, as he - as already described in this expert opinion - is not obliged to act.[100]

As mentioned above, there are no special requirements for external data protection officers. He shall be liable on a civil-law level without any special civil-law features. In the case of an agency agreement in accordance with Article 675(1) BGB (German Civil Code), as it exists with an external data protection officer, there are no special liability provisions. In principle, the external data protection officer is therefore liable according to the conditions described at the beginning. A liability privilege similar to the limited employee liability described above is not apparent.

The General Data Protection Regulation standardises - as already described under point 1.3.1 above - a large number of tasks that the data protection officer is responsible for and in doing so is not fully transparent and unambiguous in every respect.[101] Some misleading wording is to the detriment of the legal certainty of the companies and ultimately also to the detriment of the data protection officers themselves due to a certain legal uncertainty.[102] However, it is in principle up to the claimant to present and prove the facts which are to support his claim. This relative uncertainty about the tasks and duties of the data protection officer, which stems from the General Data Protection Regulation, is exacerbated by the consequences of a culpable breach of duties on the part of the internal data protection officer, which are themselves difficult to foresee in practice.

Due to the uncertainties outlined above, it may be advisable in practice to precisely define the individual tasks and duties of the data protection officer in the company in the consultancy agreement of the external data protection officer. This would achieve clarity for both

[99] Klug, ZD 2016, 315,318
[100] Cf. zur strafrechtlichen Haftung des Compliance-Officers und der entsprechenden Rechtsprechung des BGH (the criminal liability of the Compliance Officer and the corresponding jurisdiction of the BGH) below, Article 2.2.1
[101] Marschall/Müller ZD 2016, 415, 420
[102] Marschall/Müller loc. cit.

parties as to the exact tasks of the data protection officer in the company and also with regard to any breaches of obligations.

It is also possible to contractually extend the tasks and duties of the data protection officer so that the company grants him the authority to issue instructions for the performance of his tasks. However, this would then also lead to an expansion of the liability risk described here, as it would then also be subject to an obligation to act, particularly in the context of monitoring.[103] Thus, by granting authority to issue instructions, companies could also deliberately force an intensification of liability risks. It is therefore to be recommended that the data protection officer moves within the scope of his tasks as standardised by the General Data Protection Regulation - in detail concretised by contract provisions - but that, if possible, no additional powers to issue instructions can be granted, because this can lead to a civil-law shift in liability to the detriment of the data protection officer.

The external data protection officer is therefore fully liable for any damage originated causally by him unless there is a contractual limitation of liability. Point 1.3.3 still explains how to assess the damage.

In addition, any claims for damages by a data subject against the external data protection officer may also be considered. Since there is no contractual relationship between the two, only claims arising from the aspect of the contract with protective effect in favour of third parties or from tort law according to Articles 823 ff. BGB (German Civil Code) may come into question at all.

A contract with a protective effect in favour of third parties could be seen, for example, in the company's consultancy agreement with the external data protection officer. Please refer to point 1.3.1 for an explanation of the agreement with protective effect in favour of third parties. On the same grounds, a liability constellation such as this with regard to the external data protection officer should be rejected, as it cannot be seriously assumed that the contractual agreements between the external data protection officer and the company should include an unforeseeable number of data subjects in their protective effect. In particular, there is nothing of the kind in the consultancy agreement submitted.

In order to avoid repetitions, reference is also made to the remarks in point 1.3.1 with regard to claims by the data subject under tort law. There will normally be no damage caused by a breach of duty, as the data protection officer has no means of effectively enforcing his suggestions and proposals. Unlike an employee, the external data protection officer cannot invoke an analogous limitation of liability under tort law. He is liable in principle to the full extent.

[103] So probably also Marschall/Müller loc. cit.

It is therefore advisable to take out a contractual limitation of liability (see point 1.3.4 below) and/or a third-party liability insurance policy to cover this.

The question must therefore be answered in such a way that the external, designated data protection officer is liable in accordance with the relevant civil law provisions, without any intrinsic privileged liability being granted to him.

1.3.3 Question: *"Data protection officers are responsible for monitoring compliance with the GDPR. Is liability conceivable for sanctions in the event of a failure to monitor? What conditions are necessary for this?*"

Article 39(1) GDPR assigns the data protection officer primarily informational and advisory tasks as well as monitoring and cooperation tasks. This provision corresponds to the qualification which Article 37(5) GDPR presupposes. Article 39(1) lit. a GDPR correlates with the direct reporting line to the highest management level laid down in Article 38(3) sentence 3 GDPR and obliges the data protection officer to inform senior management of the company or authority about processes which are relevant to data protection. The advisory duty linked to this duty to provide information requires that the data protection officer proposes measures to comply with European and national data protection law.[104]

However, it is also the responsibility of the data protection officer to monitor compliance with the provisions of the General Data Protection Regulation and other European and national rules in the controller. This task resulting from Article 39(1) (b) of the General Data Protection Regulation certainly represents a "paradigm shift".[105]

As stated above under point 1.3.1, the internal data protection officer is liable according to the principles of employee liability set out above. If the internal data protection officer culpably breaches his obligations under the employment contract and his duties as data protection officer, he shall be liable for the damage caused by him, taking into account the principles of employee liability. In this context, however - as already mentioned above - it must be taken into account that the data protection officer has no possibility of implementing his suggestions and ideas vis-à-vis the controller either under the provisions of the currently applicable Federal Data Protection Act or under the provisions of the General Data Protection Regulation. The primary responsibility and also the final decision always lie with the controller.

It must therefore be taken into account that the data protection officer, despite his many tasks and obligations, cannot force the controller to implement the measures that would be required to comply with the rules of the General Data Protection Regulation.

[104] Klug, ZD 2016, 315, 318
[105] Marschall/Müller, ZD 2016, 415, 418

If the data protection officer culpably fails to meet his monitoring obligations in accordance with Article 39(1) (b) GDPR, a corresponding liability is, in fact, justified. However, liability would only be considered if the sanction by the supervisory authority would not have been imposed if the data protection officer had exercised his monitoring function. In structural terms, a possible liability of the data protection officer is generally linked to a failure to fulfil the tasks and duties of the data protection officer. In a case of omission, damage always results causally through the defaulter only if conduct in accordance with the standard cannot be implied without the damage incurred ceasing to exist. Consequently, the data protection officer may only be held liable for a sanction imposed by the supervisory authority if it can be proven that the controller would not have received a sanction imposed by the supervisory authority if the data protection officer had performed his duties properly. It must therefore be evident that the data protection officer's suggestions were respected in all cases by the data protection officer. Evidence of this will be difficult to provide in individual cases.

As far as the question aims at whether a fine that is imposed can be passed on, not just the causality justifying the liability (see above) but also the resulting causality underlying the liability must be considered.

It is necessary to clarify at the outset that, in the view of the authors of this expert opinion, the task of the data protection officer is not to eliminate data protection infringements from taking place despite monitoring, and that the concept of "monitoring" cannot be broadened to such an extent that it gives rise to an obligation to act which can be used to justify liability on the grounds of failure to act.

The question of whether a fine can generally be passed on internally has not been conclusively clarified. In general, it can be said that passing on a fine is only possible if it can be causally attributed to the obligations of the infringing party. In the constellations that are possible here, passing on a fine is therefore always ruled out if actions aimed at averting fines were possible, because such actions do not fall within the duties of the data protection officer.

In addition, contributory negligence on the part of the controller in accordance with Article 254 BGB (German Civil Code) may also be considered, since the controller is himself obliged to comply with data protection, as explained above. This can lead to a minimisation of the claim up to an exclusion of the liability of the data protection officer. What is decisive is the care taken by the controller himself and the extent to which he has not carried this out or not carried it out properly. It is necessary that the controller, as the injured party, has ignored the care that a reasonable person takes in his own interest in order to protect himself from the damage.[106] Since the controller is already obliged by the provisions of the General Data Protection Regulation to comply with the data protection provisions, it is possible to argue

[106] Cf. Oetker in MünchKomm BGB, 7th ed. 2016, Article 254 marginal 30

that, in the context of his organisational duty, a not inconsiderable contributory negligence can generally be assumed if the data protection officer infringes monitoring obligations. For these duties are always also obligations of the controller.

In addition, damage-promoting aspects, which are mentioned in Article 83(2) GDPR, cannot be passed on to the data protection officer due to a lack of causality, as these are not within the sphere of influence of the data protection officer. Only the measures taken by the controller to reduce the damage suffered by the data subjects pursuant to Article 83(2) lit. c GDPR are given here by way of examples.

Ultimately, the imposition of the fine should be covered by the protective purpose of the standard. Article 39(1) lit. b GDPR is designed, in the view of the authors of this expert opinion, in such a way that not every breach of data protection should be prevented. Rather, the standard is designed in a way that means breaches of data protection are brought to light by obtaining information and that these are then remedied by the controller. This means that the controller is responsible for data protection, and the data protection officer is responsible for the corresponding additional check. A fine will therefore not be covered by the protective purpose of the standard. This is particularly evident with regard to those on whom the sanctions mentioned in Article 83 GDPR are imposed.

However, this position is not uncontroversial.

According to the authors of this expert opinion, a DPO is not liable for sanctions imposed on the controller for lack of accountability due to poor monitoring by the DPO.

1.3.4 **Question:** *"Are contractual limitations of liability an option?*"

For the internal data protection officer, limitations of liability or even exclusions of liability agreed under the terms of employment contracts or supplementary agreements are easily conceivable. This applies at least to such infringements of legal obligations caused by moderate negligence. Damages caused by gross negligence or even intentionally can hardly be the subject of liability exclusion regulations agreed in advance.

However, in practice in working life, it cannot be assumed that an employer will be prepared to give a "carte blanche" from the outset to an employee taking over the post of data protection officer. As explained above, the liability of employees within the framework of the employment relationship is limited anyway on the basis of the case-law of the Federal Labour Court. In addition, liability can only be considered in the case of damage resulting causally from an omission by the data protection officer. The number of cases in which full or even merely extensive liability of the internal data protection officer will be enforced will therefore ultimately remain quite limited.

Nevertheless, considerations of offering liability insurance cover for data protection officers are likely to find fertile ground. The General Data Protection Regulation does not exclude any fundamental liability on the part of both the internal and external data protection officers. Nevertheless, this will not necessarily apply to every breach of duty; due to the fact that the breach of duty will generally result from an omission, the potential claimant will have to overcome various hurdles in order to present his alleged claims. Irrespective of this, there is also the fact that the data protection officer, despite his extensive duties, only has a compliance function to fulfil and is therefore is placed at best beside the controller, but does not accept his obligation - in particular that derived from Article 24 GDPR - and cannot therefore be prosecuted directly for this.

From a purely civil law point of view, limitations of liability within the framework of the statutory provisions are quite feasible. Article 276(3) BGB (German Civil Code) stipulates that liability for intent cannot be waived in advance for the debtor. The law does not provide for further exclusions or limitations of liability in the case of an individual contract.

If, however, pre-formulated contractual conditions are used, the additional provisions of the law of the General Terms and Conditions must be observed. This is already the case if a page uses a sample contract that is intended for multiple use, even if it is actually used only once.[107]

If General Terms and Conditions exist, these shall be measured against the special requirements of Articles 307 to 309 BGB (German Civil Code). These are intended to ensure that there is no one-sided shift in interests as a result of one party imposing its conditions on the other.

A limitation of liability is then only possible in accordance with Articles 307 to 309 BGB (German Civil Code), whereby case law critically opposes a limitation of liability and usually only approves it within narrow limits.

1.4 Appendix questions

Question: *"Do appointments made under the BDSG remain effective under the GDPR as the designation of the data protection officer*?

As already elaborated in the context of this expert opinion, the prerequisites for a mandatory designation of the data protection officer pursuant to Article 37(1) GDPR and, in particular, Article 5 BDSG-new and Article 38(1) BDSG-new are largely tied to the provisions of the currently applicable Federal Data Protection Act. There are therefore practically no conceivable case constellations in which, according to previous law, a mandatory appointment of the data protection officer had to be implemented, but under the new law no mandatory designation would have to be made.

[107] Cf. Grüneberg in Palandt, 76th edition 2016, Article 305 BGB marginal 9

Against this background, it can be assumed that the previous appointments will continue to exist as designations of a data protection officer even after the General Data Protection Regulation comes into force. In this context, the renewed consideration of the sense and purpose of the General Data Protection Regulation and also the BDSG-new is to be based on the assumption that the new introduction and entry into force of the General Data Protection Regulation will not endanger or completely reorganise the German system of data protection officers in companies and administrations. If the national legislator in Germany has already decided to ultimately retain the appointment conditions regulated in Article 4 f (1) BDSG as far as possible even under the validity of the General Data Protection Regulation, it is logical to assume that data protection officers appointed under the validity of the currently applicable Federal Data Protection Act will in principle remain in office after the General Data Protection Regulation comes into force.

In principle, appointments made under the Federal Data Protection Act continue to exist, but the duties and legal position of the data protection officer will in future be governed by the General Data Protection Regulation.[108]

1.4.1 Question: *"Are there differences between internal (employed) and external (see sample contract) data protection officers*?"

There should be no differences between internal and external DPOs as regards the continuity of previous appointments as designations under the General Data Protection Regulation.

The consultancy agreement provided as a model already ties in with the General Data Protection Regulation in Article 1. Even if the relevant consultancy agreement did not mention the provisions of the General Data Protection Regulation, it is unlikely, on the basis of the considerations set out above, that an appointment under the Federal Data Protection Act will be eliminated by the introduction of the General Data Protection Regulation. The appointments remain effective as designations. Their legal consequences will be governed exclusively by the General Data Protection Regulation from the time of its entry into force.

1.4.2 Question: *"Will implied appointments be an option through continuation of the activity?*"

As the previous appointments will continue to apply and be considered designations, implied appointments by continuation of the activity are not likely to be necessary.

[108] Jaspers/Reif RDV 2016, 61, 62

As has already been elaborated in the context of this opinion, the General Data Protection Regulation on data protection also assumes that a unilateral act, the appointment, by the controller, is required in order to obtain the post of data protection officer. An implied appointment is therefore inconceivable. In contrast to the Federal Data Protection Act, the General Data Protection Regulation does not require the designation to be in writing, but it does require an act by which the data protection officer is brought into office.

Due to the circumstances outlined above, an implied designation of a data protection officer is not necessary. Earlier appointments according to the Federal Data Protection Act remain effective as designations.

2. Criminal status of the data protection officer under the GDPR

2.1 Preliminary questions about the GDPR

Explanation of the questioner: *"The previous activity of the data protection officer typically consists of becoming active when processes are brought to him or when he gains knowledge of processes relevant to data protection, evaluating these processes and pointing them out to the management or, if prior checking of these processes was necessary, carrying them out. However, he did not have the obligation to 1. ensure (organisationally) that he was aware of all (data protection relevant) transactions and 2. monitor or even ensure the implementation of his opinion/statements.*

According to the GDPR, the controller (in the terminology of the BDSG: responsible body) has procedural/organisational duties to comply with the requirements of the GDPR (e.g. Articles 5, 12, 24, 32, 35, 36 GDPR). In contrast to the prior check according to the BDSG, the data protection impact assessment is also the responsibility of the controller."

2.1.1 **Question:** *"Is there a duty for data protection officers to obtain knowledge of processes relevant to data protection*?"

According to the understanding of the tasks of the data protection officer according to Article 39 GDPR represented in this expert opinion, these are to be understood with reference to the detailed derivation under point 1.3.0.1 to the effect that according to the General Data Protection Regulation the data protection officer is obliged, within the scope of his duty to review and control, to monitor the existing data protection organisation with regard to its compliance with data protection law and internal requirements. This results in an "observer" capacity, during the exercise of which the data protection officer reports relevant data protection processes to the controller.

Article 39(2) GDPR regulates that the data protection officer shall take due account of the risk associated with the processing operations in the performance of his duties. The risk-based approach of the General Data Protection Regulation is thus also reflected in his activities.

From this it can be concluded that the more the nature, extent, circumstances and purpose of the processing so demand, the more comprehensively and carefully the data protection officer is required to examine the data protection risks. This risk assessment shall be carried out by the data protection officer at his own dutiful discretion.[109]

In view of the risk-based approach and the data protection officer's duty to review the existing data protection organisation and to report to senior management, it is essential for the data protection officer - at least with an increasing risk appetite - to gain knowledge of processes relevant to data protection if he is to fulfil his duties effectively. As a rule, this certainly does not include the acquisition of knowledge of individual facts by means of one's own research, but rather knowledge of the basic workflow of the processes relevant to data protection that underpin the structure of the existing data protection organisation.

2.1.2 *"Does the data protection have a duty to monitor or even ensure that his instructions or specifications are followed?"*

The understanding of the term "monitoring" according to Article 39(1) lit. b GDPR represented in this expert opinion does not constitute an obligation for the data protection officer to monitor the implementation of his instructions and specifications or even to ensure this is done. As described in point 1.3.0.1.3 of this opinion, the data protection officer lacks the necessary authority to issue instructions in order to ensure effective monitoring of the implementation of his instructions and specifications by the controller in the sense of the question. Thus, he is not obliged to actively investigate possible breaches of data protection.[110] If the data protection officer, in the exercise of his observational role, discovers that his instructions or specifications are not implemented in the data protection organisational structure, he must (again) report this to the highest management level within the framework of his reporting obligation pursuant to Article 38(3) GDPR. With regard to the question of reporting intervals, i.e. the period of time that the data protection officer has to review a reaction of the company management to his instructions and specifications, reference should again be made to the risk-based approach of Article 39(2) GDPR. The higher the data protection officer's assessment of the risk in an area addressed by him and the more urgent the recommendation for action derived from it is, the faster he will have to report (again) to senior management in the performance of his duties if he finds an inadequate response to the implementation of his findings.

[109] Bergt in Kühling/Buchner, Datenschutz-Grundverordnung Kommentar (General Data Protection Regulation Commentary), 2017, Article 39 marginal 23
[110] See above under 1.3.0.1.3.

The point of reference for his findings is again the data protection organisational structure of the controller and the changes made to modify it.

On the other hand, the data protection officer does not have the authority to issue instructions in order to remedy the detected infringement himself. The data protection officer is therefore not obliged to remedy a data protection infringement himself within the scope of the monitoring.

2.1.3 Question: *"Does the data protection officer have a duty to set up a data protection organisation for his activities in addition to that which the company is required to set up (see Articles 5, 12 and 24 of the GDPR)*?"

Having regard to the opinion expressed in the present report on the concept of
"In the case of "monitoring" pursuant to Article 39(1) lit. b GDPR (cf. above, point 1.3.0.1.3), it should be noted that the data protection officer has neither the remit nor the authority to set up a second data protection organisation in order to prevent infringements of data protection provisions himself. This task is clearly assigned to the controller, who according to Articles 5, 12, 24 GDPR must take measures, keep evidence or provide information through appropriate actions according to the wording of the law.

A strong argument for this understanding is that the Commission's draft still provided for the obligation of the data protection officer to ensure documentation within the meaning of Article 28 GDPR-E.[111] The abandonment of this position within the framework of the trilogue negotiations shows that a broad understanding of the data protection officer's powers of intervention was ultimately not able to gain acceptance. The task of ensuring a certain procedure represents a clear "added" responsibility compared to the task of monitoring compliance with data protection regulations.

2.2 Criminal liability

Explanation of the questioner: *"In order to answer the following questions, only the obligations for the data protection officer resulting from GDPR - i.e. the intrinsic obligations of the data protection officer - are to be taken into account*".

Note of the authors: The conceptual question of criminal liability shall not be answered in the following in the sense of the German legal understanding, according to which criminal law on the one hand and administrative offence law on the other hand can be prosecuted. Rather, the concept of criminal liability is based on a "broad" understanding of sanctions law detached from this, so that responsibility is also taken into account from the point of view of administrative offence law.

[111] Bergt in Kühling/Buchner, Datenschutz-Grundverordnung Kommentar (General Data Protection Regulation Commentary), 2017, Article 39 marginal 5

2.2.1 Question: "*Could criminal liability apply to the designated data protection officer?*"

The sanction law under the General Data Protection Regulation only provides for fines in Article 83 GDPR, the imposition of which is the responsibility of the supervisory authorities. According to Article 83(8) of the General Data Protection Regulation, this fine procedure must be subject to appropriate procedural safeguards in accordance with Union law and the law of the Member States, including effective judicial remedies and due process. The form that the right to judicial legal protection takes is the responsibility of the procedural law of the respective Member State.[112] In addition, Article 84 of the General Data Protection Regulation gives Member States the possibility to establish other (additional) sanctions for infringements of the General Data Protection Regulation, in particular where Article 83 GDPR does not provide for a fine for such infringements.

The German legislator has made use of this in Chapter 5 of the new Federal Data Protection Act in the form of Articles 41 to 43 BDSG-new, which comes into force on 25 May 2018.

The Federal German provisions of the Administrative Offences Act and the General Laws on Criminal Proceedings shall apply mutatis mutandis to the punishment of and proceedings in respect of an infringement pursuant to Article 83(4) to (6) GDPR through Article 41 BDSG-new.

By means of Article 42 BDSG-new, the Federal German legislator makes use of the possibility of sanctions according to Article 83 GDPR to create a criminal offence. In Article 43 BDSG-new, an administrative offence is created in addition to the sanctions provided by Article 83 GDPR.

This leads to the question of the criminal liability of the designated data protection officer according to two case groups:

If the data protection officer leaves his intended role and deliberately commits unlawful breaches of data protection or acts as a result of a joint project in deliberate and wilful cooperation with a person authorised to make decisions by the data controller or the processor, the data protection officer may be held criminally liable for deliberate and intentional breaches in the form of perpetration or complicity through active action or aiding and abetting. However, these are likely to remain absolute exceptions.
The second case group comprises cases in which an accusation could be made against the data protection officer to the effect that he omitted a certain act and thereby (co-)caused the data protection infringement. A responsibility by omission contrary to duty is possible thereby both with criminal offences and with misdemeanours.

[112] Nemitz in Ehmann/Selmayr, Datenschutz-Grundverordnung (General Data Protection Regulation), 2017, Article 83 marginal 11

In both cases, several conditions must be met in order for there ultimately to be a possibility of punishment in the form of an offence being committed by omission:

- **Causality**

First of all, it is highly probable that the infringement would have ceased to exist had the data protection officer performed the objectively necessary act. It is necessary to demand concrete indications here that senior management, to whom the data protection officer is obliged to report, would actually have followed the proposed measure. A mere increase in the risk of an infringement through the omission of the data protection officer is therefore not sufficient to establish the causal link.[113] Since the authority of the data protection officer will always be less than that of senior management, an overall responsibility for the decision behaviour according to the principles of a cumulative omission[114] cannot be assumed here.

- **Guarantor status**

If a causal link can be established in an individual case, the next prerequisite to examine would be the existence of a guarantor status within the meaning of Article 8 OWiG (Administrative Offences Act) or Article 13 StGB (German Criminal Code). The following applies in this respect:

It was already mentioned in point 2.1.2 that, according to the understanding of the term "monitoring" as advocated by the authors of this expert opinion, there is an obligation to review the organisational structure under data protection law. This structure must be set up by the controller in accordance with the provisions of Articles 5, 12, 24 GDPR.

The understanding derived in this way of the task of monitoring pursuant to Article 39(1) lit. b GDPR must then be examined as to whether this establishes a position of guarantor for the data protection officer. In the literature so far, at least, the prevailing view represented up to now, according to the currently valid Federal Data Protection Act, was that no guarantor position resulted for the data protection officer, in comparison with the decision of the Federal Court of Justice,[115] with which in principle a guarantor position was assigned to the Compliance Officer.
In order to be able to make an accurate assessment of the duties of the data protection officer pursuant to Article 39 GDPR, a detailed examination must first be carried out of the considerations of the Federal Court of Justice regarding the transfer of duties and any resulting guarantor position. The relevant key messages of this decision are as follows:

[113] BGH, jurisdiction dd. 12.1.2010 - 1 StR 272/09
[114] BGH, jurisdiction dd. 6.7.1990 - 2 StR 549/89
[115] BGH, jurisdiction dd. 17.7.2009 - 5 StR 394/08

- By assuming obligations, legal liability in the sense of Article 13(1) StGB (German Criminal Code) can be justified, which leads to culpability owing to failure to comply with the obligations. This is based on the consideration that those to whom duties of care for a particular source of danger are delegated also have a special responsibility for the integrity of the area of responsibility assumed by them. To this end, it is first of all necessary to determine the area of responsibility which the obliged person has assumed, whereby it is not the legal form of the transfer of obligations that is important, but the content of the obligation, taking into account the legal background.

- The justification of the guarantor position can be derived from the assumption of a certain function (e.g. radiation protection officer) or from a service contract. In the latter case it does not depend on the conclusion of the contract, but on the actual assumption of the obligations.

- However, not every transfer of obligations constitutes a guarantor position in terms of criminal law. In addition, a special relationship of trust must normally be established, which induces the transferor to assign special duties of protection to the obligor. In order to determine the content and scope of the guarantor's obligation, the direction of the transfer must be taken into account. If the assigned duties consist solely in optimising internal processes and uncovering and preventing breaches of duty directed against the company, the responsibility does not go as far as if further duties are added, according to which the data protection officer must also object to and prevent breaches of law emanating from the company.

The acceptance of a guarantor position within the meaning of Article 13(1) StGB (German Criminal Code) is supported by further obligations, in particular the obligation assumed towards company management to prevent infringements of the law and in particular criminal offences through pro-active involvement.

According to the above-mentioned understanding of the task of monitoring pursuant to Article 39(1) (b) GDPR derived from the authoritative English term "monitoring", it can be assumed for the area of responsibility of the data protection officer, as determined by the obligations arising from the General Data Protection Regulation, that no position of guarantor can be derived from these original obligations alone.

However, this assessment only applies in the event that the data protection officer's actual understanding of his duties is strictly oriented along the tasks standardised in Article 39 GDPR. As soon as the data protection officer takes on an extended range of duties - in actual practice or by contractual assumption - the risk of being seen as a guarantor in the context of an assessment examining the individual case increases for him.

In summary, with regard to criminal liability, it can be stated that in rare exceptional cases this will be the case if the data protection officer deliberately and actively infringes his duties.

Theoretically, there is also a risk in the question of responsibility (criminal law or administrative offence law) for the case of omission - i.e. failure to act in breach of duty - which is relevant to practice. In this case, Article 84 GDPR not only provides for the possibility of an offence under Article 42 BDSG-new by omission but also for the risk of committing an administrative offence by omission. On the one hand, through Article 84 GDPR in the form of Article 43 BDSG-new. On the other hand, however, also in accordance with Article 83 GDPR through Article 84 GDPR and the provisions of the German Administrative Offences Act (OWiG) in the form of aiding and abetting offences by omission. This will be discussed in more detail in point 2.2.2 below.

Excursus: Article 203 StGB (German Criminal Code)

The prescription of 203 StGB is to be seen only marginally as a further sanction risk in the criminal law sense.

Even before the entry into force of the General Data Protection Regulation, there was a risk that the betrayal of secrets would be punishable under Article 203 (StGB) of the Criminal Code. This has not been mitigated by the provisions of the General Data Protection Regulation. On the contrary, Article 38(4) of the General Data Protection Regulation will increase the risk of criminal liability under Article 203 of the Criminal Code. For an internal data protection officer of a company who is not already considered as an active party pursuant to Article 203(1) or (2) StGB, an offence may arise from Article 203(2a) StGB in the case of deliberate action if this person makes an unauthorised disclosure of a third-party secret, which was entrusted or became known to a third party (holder of the secret within the meaning of paragraphs 1 and 2), and of which he has gained knowledge in the performance of his duties as data protection officer. The risk of criminal misconduct will increase even further because the data protection officer is required under the General Data Protection Regulation to monitor compliance with data protection regulations and not merely to work towards compliance as has been the case to date.

2.2.2 **Question:** *"Does the GDPR impose sanctions on the designated data protection officer? Which of his obligations are directly penalised by the GDPR?"*

No infringements, whether intentional or through negligence, against obligations incumbent on the data protection officer under Article 39 GDPR are punishable under Article 83(4) to (6) GDPR. Insofar as the prescription of Article 39 GDPR is mentioned in Article 83(4) lit. a GDPR, it is limited to the obligations of the controllers and the processors. These are the target groups of the punitive measures.[116] Consequently, the General Data Protection Regulation does not contain any obligations directly penalising the data protection officer.

[116] Nemitz in Ehmann/Selmayr, Datenschutz-Grundverordnung (General Data Protection Regulation), 2017, Article 83 marginal 40 ff.

However, the legal construct of participation in an administrative offence described above in point 2.2.1 can also indirectly be used to penalise the data protection officer.

According to the view expressed in this expert opinion, the standardised duties of the data protection officer extend to reporting to senior management and audits of the data protection organisational structure introduced and implemented by the controller. The obligation to report has taken place in proper application of Article 39(2) GDPR. The more critical the nature of the data processed, the larger the scope, the riskier the circumstances and the wider the purpose of the processing, the more closely the reporting must be made to senior management. Further obligations, such as actively investigating data protection infringements or remedying established infringements, do not affect the data protection officer in terms of the tasks assigned to him by the General Data Protection Regulation. In this respect, a more extensive range of obligations can only result from an individual contractual transfer or a de facto different handling of his role in the company by the data protection officer.

Insofar as it is also a decisive factor for determining the position as a guarantor that the duties incumbent on the data protection officer should also serve precisely to protect the infringed legally protected right (here, clearly, data protection), no separate discussion is required. This is obvious.

As regards the role of guarantor, understanding of the tasks of the data protection officer in this expert opinion, in particular the role of “monitoring”, does not imply that the duty of guarantor goes beyond proper reporting to senior management. Accordingly, a more far-reaching guarantor status only arises if the data protection officer is granted further duties and powers (command and decision-making powers) by way of delegation. Here, the assumption of a position as "monitoring guarantor" is obvious. It should be noted that, in addition to a delegation agreed in an individual contract, the actual exercise of the powers with the approval of company management will also be sufficient in this respect to be able to assume a corresponding position of monitoring guarantor.

The more far-reaching approach to the position of the data protection officer as a guarantor, according to which even without command and decision-making powers and by virtue of his enormous information and knowledge advantage and the possibility of involving the supervisory authority, he would have a position as a monitoring guarantor,[117] is to be rejected as too far-reaching.
A special case of the guarantor position is the breach of duty of prior conduct (ingerence), which with regard to the reporting obligation may result from incorrect or omitted reporting. The guarantor's position, however, only extends in this respect to the source of danger

[117] Marschall, ZD 2014, 66, 68

created by the breach of duty,[118] i.e. the inaccurate part of the data protection officer's statements in the context of his reporting.

Once the position of guarantor has been established, the failure to act in breach of duty accused in each case must also have led to a causal breach of data protection law. As a matter of principle, the comments on causality as made in the preliminary remark in point 1.3.0 of this expert opinion shall apply. It is therefore necessary to compare the actual causal course with the hypothetical course which would have resulted if the data protection officer had acted correctly. As far as the criminal-law assessment is concerned, it must be seen in this respect that in the area of aiding and abetting offences by omission, fewer demands on the part of the courts are made on causality by omission than is the case with perpetration by omission - the absence of success with the offence with a probability bordering on certainty.[119]

However, for the data protection officer, criminal responsibility for the question of causality testing may fail because of the question of legitimate alternative conduct. According to case-law,[120] causality and the attribution of success do not apply if the factual success (here: infringement of data protection) would have occurred even without the additional necessary action of the data protection officer. It is therefore necessary to determine how senior management would have reacted if the data protection officer had reported to them. In addition to the statutory provisions of the General Data Protection Regulation, internal regulations between the company management and the data protection officer will also have to be taken into account in this context, insofar as they contain instructions for his reporting. If there are doubts as to whether the breach of data protection law would also have occurred if the data protection officer had reported properly, the principle of "in favour of the accused" applies in criminal law - in contrast to the question of civil liability - so that, in case of doubt, the necessary causality no longer applies.

Finally, the data protection officer must also have acted intentionally as a guarantor in view of his failure to act. Although the uniform offender concept of Article 14 OWiG (Administrative Offences Act) applies to administrative offence law, the requirement of the double intention to assist[121] is also recognised by the case law here in order to avoid unfair unequal treatment between criminal law and administrative offence law. Conditional intent[122] suffices in this respect for the alleged omission. For this to be accepted, it is sufficient that he is aware of the general risk of an as yet unspecified data protection infringement through his omission. His motive for inaction is irrelevant. This may also be due to the desire to avoid conflict with senior management. An assumption of the weakest form of intent - conditional intent (dolus eventualis) – is not precluded if the data protection officer does not wish success (breach of data protection law) or even expressly disapproves of it.

[118] BGH, jurisdiction dd. 17.7.2009 - 5 StR 394/08
[119] BGH, jurisdiction dd. 16.1.2008 - 2 StR 535/07
[120] OLG Stuttgart, jurisdiction dd. 19.6.2012 - 20 W 1/12
[121] BGH, jurisdiction dd. 14.2.1985 - 4 StR 27/85
[122] BGH, jurisdiction dd. 18.4.1996 - 1 StR 14/96

For possible penalisation of the data protection officer according to Article 83 GDPR in connection with the provision of Article 14 OWiG (Administrative Offences Act) via Article 84 GDPR, it must be taken into account that administrative offence law only knows the term "uniform offender". In contrast to the area of criminal law in which a distinction is made between perpetrators and participants, administrative offences law only knows the uniform concept of perpetrator. By simplifying Article 14 OWiG, it is possible that even those who are not the target group of this provision may also be the perpetrator of an administrative offence. Under Article 14 OWiG, the data protection officer could also be the conceivable perpetrator of an administrative offence within the meaning of Article 83 GDPR, because Article 14(1) sentence 2 OWiG stipulates that the possibility of punishment also exists if the particular personal characteristic is only present in the case of one participant (here: controller).

However, this broad possibility of punishment is corrected by the fact that, with regard to intent, the requirements that apply in the area of criminal law to forms of participation in instigating and aiding and abetting are required to the same extent[123]. The data protection officer would therefore have to have an intention himself, both in terms of his own contribution to the offence (helping the controller to commit an offence) and in terms of the intentional offence committed by the controller. The causality of the participation requires that the data protection officer must have objectively promoted or facilitated the act of the controller through his contribution.

In conclusion, it must be stated in summary that it is highly unlikely that the data protection officer will be held responsible under sanctions law if he acts within the scope of his duties pursuant to Article 39 GDPR. According to the view expressed here, the scope of obligations under Article 39 GDPR does not include any guarantor status required for a sanction due to failure to comply with an obligation.

However, the risk of sanctions increases for the data protection officer to the extent that - as a result of individual contractual provisions or de facto handling approved by company management - he expands his scope of duties. The more he assumes command and decision-making powers, the more likely he is to be awarded a guarantor position in the event of his failure to act in accordance with his duties.

2.2.3 Question: "*Does the designated data protection officer have a general duty to prevent breaches of data protection within the company*"?

Again, the obligations defined for the data protection officer must be taken into account. A general obligation to prevent data protection infringements in the company in the form of an active duty to take action cannot be seen here.

However, the obligation to monitor the organisational structure under data protection law and the more extensive reporting obligation to senior management level mean that there is an indirect obligation to monitor the instruments provided by the company to prevent data protection infringements.

[123] OLG Düsseldorf, jurisdiction dd. 31.8.2001 - 2a Ss 149/02-46/01 II

Here, too, it is necessary to recall the risk-based approach standardised in Article 39(2) GDPR, according to which the data protection officer in his independent position must carry out the risk assessment himself according to his dutiful discretion.

The prevention of breaches of data protection can, however, only refer in this respect to reviewing the organisational structures introduced by the controller, which are intended to prevent a breach of data protection provisions. However, active intervention to eliminate or prevent individual infringements should not be regarded as part of the data protection officer's duties in the absence of appropriate powers of instruction. This could, if necessary, be done by means of a corresponding individual contractual agreement between the controller and the data protection officer with regard to his powers.

It has been decided under constitutional law that only a purely de facto possibility of averting success or moral duties cannot constitute a guarantor,[124,] which is why the question is based exclusively on the scope of duties of the individual case to be assessed.

2.2.4 Question: *"Does the designated data protection officer have an obligation to prevent certain data protection breaches within the company*?"

For the reasons stated in point 2.2.3, an obligation to prevent certain breaches of data protection must also be negated.

2.2.5 Question: *"Control tasks are one of the main obligations formulated for data protection officers. Can sanctions result directly from a lack of checks within the company?*"

As described above under point 2.2.2, the data protection officer is exposed to the risk of sanctions due to a lack of control in the company by participating in an administrative offence based on his failure to comply with his duty.

The monitoring of the data protection organisation structure of the controller can therefore lead to a sanction under the conditions listed there. In addition to Articles 41 to 43 BDSG-new, the possibility of sanctions is also opened up by the possibility of sanctions under administrative offence law pursuant to Article 83 GDPR in the form of participation through non-compliant omission.

[124] BVerfG, jurisdiction dd. 21.11.2002 - 2 BvR 2202/01

2.2.6 **Question:** *'Does the designated data protection officer have an obligation to prevent data protection breaches within the company if he has previously pointed out the illegality*?

The view expressed in this expert opinion is that there is no obligation to prevent data protection infringements. As already stated several times in this expert opinion, the obligation is limited to reporting to the management of the controller.

If the data protection officer has already pointed out an unlawful situation discovered by him in the course of his reporting, it is, however, incumbent upon him, against the background of Article 39(2) GDPR, to pay particular attention to the situation discovered and any reactions of the controller to it in the course of his future reporting. If the data protection officer no longer pays attention in future reporting to the circumstances which he has already criticised, this may result in an unlawful breach of duty and an associated breach of the guarantor's position.

2.2.7 **Question:** *"Is there a difference between whether the DPO is an employee of the company or an external service provider?*"

With regard to the question of the quality of the perpetrator in terms of criminal law or administrative offences, it is irrelevant whether the data protection officer is an employee of the company or an external service provider. Such a distinction is not made according to the norms of criminal law or administrative offences law. The only decisive question is whether the officer can be held responsible as a perpetrator or as an assistant (criminal law) in a specific individual case.

In each case, the duties assumed by him and any further powers assigned to him by individual contracts shall be taken into account.

2.3 Delegated tasks

Explanation of the questioner: *"The previous practice under the BDSG suggests that the controller will transfer certain tasks of the GDPR to the data protection officer - at least de facto*".

2.3.1 **Question:** *"For criminal liability, is it necessary to distinguish between, on the one hand, the original duties of the data protection officer and, on the other, duties assumed by delegation*?

With regard to the question of the consequences of sanctions, it is not necessary to distinguish between infringement of the primary tasks of the data protection officer or infringement of assumed duties. A sanction is always imposed if the breach of duty fulfils the criminal law requirements for the assumption of a guarantor position as well as the other conditions of the evidence.

However, as already mentioned above (point 2.2.2), responsibility resulting from the primary tasks of Article 39 GDPR is unlikely to arise in the event of careful reporting in the absence of further instruction and decision-making powers on the part of the data protection officer.

Insofar as further duties and powers are conferred on the data protection officer by delegation, the latter's risk of being held criminally responsible in the event of accusable non-fulfilment of these duties also increases.

Point 2.2.1 states to the extent that it is decisive whether the data protection officer's delegated authority - contractual or factual - authority also includes, in addition to reporting, the right to take targeted action against individual infringements by issuing instructions and taking action, or to prevent such infringements on an individual basis. According to the legal view expressed in this expert opinion, the General Data Protection Regulation does not provide for this power. If, however, the data protection officer allows supplementary tasks to be assigned to him, the implementation of which also involves the assignment of extended rights (right to issue instructions and decision-making authority) to him, his responsibility will also come to the fore under criminal law if he does not exercise the decision-making leeway assigned to him or does so contrary to his duties.

In this respect, the provision of Article 38(6) GDPR, according to which the data protection officer may perform other tasks and duties, is of particular importance. However, the question to what extent and in what area the assumption of further obligations under this standard increases the risk of criminal liability is not covered by the given question. Here too, the principle will be that Article 38(6) GDPR must be observed for the determination of the concrete scope of obligations. This goes hand in hand with the fact that the assumption of a task which infringes Article 38(6) of the General Data Protection Regulation is associated with an increase in the risk under sanctions law.

2.3.2 **Question:** *"When does the data protection officer incur criminal liability for delegated tasks? Is the form of delegation of the task relevant for this?*"

With regard to the risk of increasing criminal liability inherent in a delegation, reference is made to the remarks under point 2.3.1. If an extended remit is transferred within the framework of the delegation, it should be clearly defined from the point of view of the data protection officer as to how far his powers extend in order to best avoid risks. In the case of particularly risky transfers of tasks, the final decision-making authority should remain with the company management. In his own interests, the data protection officer must document that this has been obtained.

If the data protection officer has concerns about the legality of the implementation he favours when carrying out his delegated tasks, he should seek contact with the supervisory authority on his own initiative in order to avoid a criminal risk.

Berlin, 31.07.2017

Derra, Meyer & Partner PartGmbB
RA Konrad Menz

APPENDIX 1

Appendix 1 - Tips for action on important aspects:

- Do not assume any authority, as this may lead to an extension of liability.

  The data protection officer of the company is not liable for any omission with regard to the obligations under the General Data Protection Regulation, because due to his lack of scope for action he is not obliged to independently remedy a data protection infringement. However, if he is given authority with which he could end the data protection infringement, the question of the duty to act arises anew. Whether this duty to act is based on this, has not been, but there is a liability risk that cannot be calculated at this point in time.

- Take out professional liability insurance.

  This is not mandatory for external data protection officers, since the contract is a service contract which does not in itself provide for such insurance (unlike, for example, doctors or lawyers). Unlike the internal data protection officer, the external data protection officer has no liability privileges. For this reason, it is advisable for the external data protection officer to have appropriate liability insurance in addition to a contractual limitation of liability to the sum insured.

- No obligation to recast or amend existing contractual arrangements

  The General Data Protection Regulation and the BDSG-new do not lead to a change in the status and basic legal relationship of the data protection officer. There is therefore no immediate need to conclude new contractual agreements, such as a new work or service contract, on the basis of the changed legal framework alone. Nevertheless, it is advisable to review existing contracts for any need for adjustment, as from 25 May 2018 only the provisions of the General Data Protection Regulation and the BDSG-new will apply; the current Federal Data Protection Act no longer applies, not even for a transitional period.

- Definition of individual tasks and duties in the employment contract

  Due to legal uncertainties, it is advisable to precisely define the individual tasks and duties of the data protection officer in the company in an original employment contract of an employee recruited as data protection officer or within the framework of an agreement on the assumption of the position of data protection officer (in the case of a subsequent designation as data protection Officer).

- Consideration of own interests

In order to avoid a personal sanctions or liability, the data protection officer must take his own interests into account when performing his duties. If he does not have sufficient capacity to perform his duties or if he finds that the statements made in his reports to senior management are not taken into account, he will have to present these circumstances again and again in a continuous reporting process. If he is not sure about the assessment of the factual or legal situation, he must point this out and propose obtaining further expertise. If he is offered the delegation of tasks by the most senior management level, which increases his liability for legal sanctions or legal liability for risk, he should reject this form of delegation with appropriate justification. If, on the other hand, the data protection officer decides to assume the tasks to be delegated, he is strongly advised to regulate this contractually and to obtain insurance cover for the extended tasks. In any case, the delegation shall ensure that the additional tasks do not lead to a conflict of interest with the primary tasks of the data protection officer.

APPENDIX 2

Sample agreememt - not to be used

(based on the old legal situation)

Certificate of appointment

of an external data protection officer according to Article 4 f BDSG (Federal Data Protection Act)

The company ...

represented by (management / board of directors),
and/or on behalf of individual executive management

boards, appoints with effect from (date),

Ms/Mr ... to be external data protection officer according to Article 4 f BDSG / Articles 37, 38 EU-GDPR in his capacity as an employee of xy management consultancy.

Ms/Mr ... is hereby appointed as deputy.

The tasks and obligations resulting from this appointment arise from the BDSG up to 24th May 2018, in particular from Articles 4f, 4g, and from 25th August 2018 from the EU General Data Protection Regulation, here in particular Articles 38, 39, and are not listed separately here. In this function, the data protection officer according to BDSG reports directly to the board of directors / company management.

The appointment is made as a supplement to the consultancy agreement from the date listed. The appointment ends automatically when this agreement is terminated.

All other issues are regulated in the above-mentioned agreement on the appointment of the data protection officer and apply in equal measure.

Place1, Date

Place2, Date

_____
Management / Representative

_____
Data protection officer/
Management

APPENDIX 2

Sample - not to be used

(based on the old legal situation)

Consultancy agreement

The following **consultancy agreement** is concluded between

the company
- hereinafter referred to as the Client - represented by: (Board of Directors / Managing Director)

and

the Consultant (Managing Director)

1 Subject matter and scope of the order

The object of the Consultant's service is to act as the company data protection officer within the meaning of Article 4 f (1) of the Federal Data Protection Act (BDSG) or, as applicable, from 25 May 2018 within the meaning of Article 37f (EU-GDPR) of the EU Data Protection Act with the statutory duties pursuant to Article 4g of the BDSG or pursuant to Article 39 of the EU-GDPR.

The Consultant undertakes these tasks for the Client in the following company:

- ❒ *...list legally independent companies*
- ❒ *…*

In performing this task, the Consultant shall be assisted by internal contact persons. They shall ensure communication and information and support the organisation of appointments.

This agreement does not constitute a contract in favour of third parties within the meaning of Article 328 BGB (German Civil Code). It is the responsibility of the Client to ensure that the necessary contractual and actual prerequisites for the Consultant to perform his or her tasks are met by any associated companies.

2 Provision of services

(1) The time and place of the assignment for the Client shall be freely determined by the Consultant. If urgent matters require immediate discussion or examination, the Consultant shall also be available at short notice, whereby consideration shall be given to his other operational requirements to the extent that these may not be unreasonably impaired thereby.

(2) The Consultant shall be entitled to employ suitable employees and competent third parties for the execution of the matters assigned to him. The Consultant's own responsibility remains unaffected by this.

(3) The Consultant shall carry out his activities on his own premises. Insofar as the execution of the appointment requires a presence at the Client’s premises or at one of the offices listed in Article 1 is required, the Client shall, after prior consultation with the Consultant, ensure that the necessary operational facilities are made available to the Consultant at the premises of the Client or the respective company.

3 Duty of confidentiality

(1) The Consultant shall be obliged in accordance with the law to maintain confidentiality with regard to all matters of the Client or other companies pursuant to Article 1 which come to the attention of the Consultant during or on the occasion of the execution of an order, unless the Consultant has been released from this obligation in writing by the company concerned.

(2) The duty to confidentiality does not apply if the disclosure of matters is absolutely necessary to safeguard the Consultant's legitimate interests. The Consultant shall also be released from the duty of confidentiality insofar as he is obliged to provide information and to cooperate in accordance with the terms of a liability insurance policy.

(3) The statutory rights to information and the right to refuse to make statements shall remain unaffected by the above provisions, as shall the Consultant's special obligations to confidentiality pursuant to Article 4f (4), 4a BDSG.

(4) This duty of confidentiality on the part of the Consultant shall continue to apply even after termination of the contractual relationship. Reports, expert opinions and other written statements made on the basis of or on the occasion of this order may only be handed over by the Consultant to third parties with the consent of the Client, except in the case described in Article 3(2) sentence 2.

(5) To the same extent as for the Consultant himself, the duty of confidentiality also applies to the employees, partners and assistants.

(6) If the Consultant calls in expert third parties, he shall ensure that they are bound to confidentiality to the same extent.

4 Liability

(1) The Consultant shall be liable for his own negligence and for the negligence of his own employees and assistants.

(2) The Consultant has taken out liability insurance with an insured sum of €1,000,000 per individual case. He undertakes to maintain the insurance cover in this amount for as long as this contractual relationship exists.

(3) Should a higher liability amount be required in an individual case, the Consultant and the Client shall discuss this and decide whether a higher insurance sum should be concluded with the liability insurance for this individual case. The costs of a higher insurance sum shall be borne by the Client.

(4) Insofar as a claim for damages by the Client vis-à-vis the Consultant is not subject to a shorter limitation period by law, it shall become statute-barred three years after the date on which it arose. The claim must be asserted within three months of the Client becoming aware of the damage.

5 Limitation of liability

In the event of slight negligence in a liability case, the Consultant may only be held liable by the Client up to the amount of the existing minimum sum insured in accordance with Article 4. Any liability on the part of the Consultant for further damage is hereby expressly excluded.

6 Exclusion of liability

Any liability is excluded for verbal information outside of an agreed consultation or telephone information. This does not apply if the information is confirmed in writing with the facts described by the Client.

7 Remuneration

(1) As a lump-sum fee, a monthly amount of

(see quotation) € plus the statutory value added tax applicable at the time.

is agreed. In this agreement, the parties assume that the Consultant's monthly expenditure of time for the Client, including all companies pursuant to Article 1, does not exceed an average of *8 hours.* This cost estimate is based on the standard model, which includes the usual tasks according to BDSG.

Should it turn out in the course of the annual planning discussion that the expenditure is insufficient or that an adjustment of the expenditure of time is necessary due to projects or other tasks, the parties will agree on the adjustment of the fee.
If necessary, travel (train or flight) and accommodation costs will be charged at cost price. A flat rate of €0.50 per km (plus applicable VAT) from the nearest office is charged for travel costs by car *(see quotation)*.

(2) In addition to the monthly expenditure specified under 7(1), a one-off expenditure for the inventory is agreed at a fixed price of *(see quotation)* € plus applicable value added tax.
The project expenditure for the implementation of the short-term tasks required according to the appraisal is initially estimated at *(see quotation)* days and agreed at a daily rate of € *(see quotation)* plus applicable VAT.
This expenditure serves the initial implementation of data protection in the processes and regulations, the creation of guidelines and a data protection concept as well as the initial inclusion of the procedural documentation.

(3) The following activities of the Consultant shall not be included in the lump-sum fee and shall be remunerated separately, if applicable:
- IT-security support
- Project tasks that cannot be processed within this scope (introduction of new software, foreign locations, company growth, etc.)

(4) Activities in accordance with section (3), will only be carried out after consultation with the Client. For these activities, a fee of *(see quotation)* € per hour or part thereof plus applicable value added tax is agreed.

(5) The payment of the monthly flat fee is due on the 15th of the respective calendar month. Other expenses and fees for additional activities pursuant to sections (2) and (3) shall be charged separately by the Consultant at the end of each month.

(6) All amounts shall be transferred to one of the following accounts:

Account holder:

BIC
IBAN
Bank:

VAT
no:

8 Duration of contract

(1) The contract begins on *(see quotation)*.

(2) The contract has a limited term of two years and can be terminated for the first time on xxx with notice of six months. If the contract is not terminated, it shall be extended by a further two years.

(3) Notice of termination must be given in writing.

(4) In all other cases, the provisions of the BGB (German Civil Code) apply to the termination of the contract.

9 Cooperation of the Client / Certificate of appointment

(1) The Client is obliged to cooperate in the execution of the appointment to the extent necessary for proper execution of the appointment. He shall provide the Consultant with all evidence, certificates and other documents required for the execution of the appointment in connection with the matters to be processed by the Consultant for inspection and perusal, and shall provide the Consultant with the information necessary for clarifying the facts of the case, in particular with an overview of procedures within the meaning of Article 4 e sentence 1 BDSG (cf. Article 4 g (2) sentence 1 BDSG), insofar as the preparation of the overview is not a task within the scope of this agreement (cf. 7.2).

(2) Furthermore, the Client shall inform the Consultant comprehensively about the factors and backgrounds which are essential for the assessment of the facts of the case. He shall inform the Consultant of all operational procedures and circumstances which may be relevant to the performance of the agreement.

(3) The certificate of appointment shall be presented by the Client after conclusion of this agreement and signed by both contracting parties.

(4) The Client is responsible for ensuring that any other companies/locations also meet the aforementioned cooperation obligations in the same way and that the respective certificates of appointment are issued.

10 Amendments/Additions

There are no verbal ancillary agreements. Amendments or additions to this contract must be made in writing.

11 Severability clause

Should individual provisions of this agreement be or become invalid, this shall not affect the validity of the remaining agreements. The contracting parties undertake to replace ineffective provisions by provisions which come as close as possible to the original purpose and whose effectiveness does not meet with any objections. The same shall apply in the event of gaps in the contract.

Place, Date	Place, Date
_____	_____
For the Client	Consultant