DATA PROTECTION SUPERVISORY AUTHORITY OF JEHOVAH'S WITNESSES

Data Protection

2019 Activity Report

2019 Activity Report

From the **Data Protection Supervisory Authority of Jehovah's Witnesses**

The **Data Protection Supervisory Authority of Jehovah's Witnesses** must present an annual report on its operations to the Branch Committee and the public (§ 24(6) Data Protection Act of Jehovah's Witnesses). This report covers the period from June 2019 to December 2019.

IMPRINT

Publisher: **Data Protection Supervisory Authority of Jehovah's Witnesses**

Grünauer Straße 104
12557 Berlin
Telephone: +49 (030) 65481080
Email: datenschutzaufsicht@jehovaszeugen.de
Website: www.datenschutz-jehovaszeugen.de

Presented in December 2020

CONTENTS

NOTE:

The Glossary (at the end of the Activity Report) provides explanations of various specialised terms. When the first appearance of a term is highlighted in a different colour in the main text (for example, personal data), this indicates that a more detailed explanation is available in the Glossary.

INDEX OF ABBREVIATIONS

BDSG	German Federal Data Protection Act
DSGJZ	Data Protection Act of Jehovah's Witnesses
GDPR	General Data Protection Regulation of the European Union
EU	European Union
CJEU	Court of Justice of the European Union
K.d.ö.R.	Corporation under public law
StRG	Statutes of the Religious Association: Jehovas Zeugen in Deutschland
VersO	Congregation Charter of Jehovah's Witnesses

Introduction

With the introduction of the General Data Protection Regulation (GDPR) that applies throughout Europe, data protection did not achieve its objective, but only really got it started. Parallel to this, the revised Data Protection Act of Jehovah's Witnesses (DSGJZ) has strengthened the rights of all data subjects. We hereby present the 2019 Activity Report in order to document the work of the **Data Protection Supervisory Authority of Jehovah's Witnesses** in accordance with European legal regime.

The 21 May 2018 version of the DSGJZ has been in force since 24 May 2018 and is bringing unprecedented attention to data protection, as reflected in the number of review requests, information requests, erasure requests, and requests for advice and training.

Hence, our experience in 2019 is that the rules on data protection have arrived, are effective and continue to uphold the level of data protection for all data subjects. We are therefore confident that the DSGJZ is effective – through clearly defined rules such as the right to access information, the right to rectification, the right to erasure, and the right to restriction of processing.

Furthermore, we were able to determine in 2019 that the inquiries for advice on data protection issues have not decreased, but have significantly increased instead. Our core function is to advise data subjects and those responsible for data processing [controllers] within the religious association and to promote public awareness about data protection issues.

We take this objective very seriously, since data protection will only really be successful for all if everyone has a share in it – either actively, by understanding and implementing basic data protection standards, or passively, by participating in the regulations and rights arising from data protection.

Article 91 GDPR is still authoritative, serving as an interface and simultaneously as a bridge between the ever-evolving data protection law of the European Union and the religion's own rules.

However, for the religious association **Jehovas Zeugen in Deutschland, K.d.ö.R.**, the protection of personal rights was always based on the view of mankind that the religious association and its members derive from their understanding of the Bible. Great importance has always been placed on maintaining strict confidentiality regarding the personal circumstances of the individual – especially from the point of view of the pastoral relationship of trust (Proverbs 20:19; 25:9).

Pastoral activity always presupposes that each faithful adherent can freely disclose and openly express problems (Proverbs 15:22). The need to protect privacy is a prerequisite for the realisation of fundamental principles of the religious association (§ 14(1) StRG, § 3(5) subparagraphs 1, 2 VersO).

Therefore, the religious association has been making provisions in its ecclesiastical law for decades to ensure that personal data is protected — even before data protection laws were established at the regional, national, and European Union levels. The decades of bitter persecution under the National Socialist regime and the German Democratic Republic (East Germany) taught Jehovah's Witnesses the importance of protecting privacy and of not disclosing personal data. The persecution, bans and deprivation of rights which persist in some parts of the world give rise to the need for a global standard to safeguard confidentiality.

Regardless of the legal forms of the religious association's various structural divisions and agencies (§ 5 StRG), all are subject to the ecclesiastical law (Preamble, paragraph 4 StRG). This forms the basis for the actions of the religious association. The preservation of each individual's right to privacy is guaranteed by means of the religious association's own appropriate data protection policy. This Data Protection Act of Jehovah's Witnesses (DSGJZ) was adopted on the basis of the constitutionally guaranteed right of **Jehovas Zeugen in Deutschland** to independently organise and administer its affairs within the limits of the laws that apply to all. This right is also respected under European Union law and laid down in Article 91 and recital 165 of the GDPR and Article 17 of the Treaty on the Functioning of the European Union (TFEU). In exercising this right, the current version of the DSGJZ is compatible with the GDPR.

It must be clear to everyone, whether data subject or data controller, that data protection is not an irritating burden, nor is it superfluous bureaucracy, but rather, the prerequisite for the fair and transparent handling of the right to self-determination with regard to information.

Therefore, data protection is not created by a supervisory authority, but only by the understanding and acceptance of each individual user and processor of data. Data protection thus begins with each data subject, who knows and exercises his rights. The understanding and sense that data protection concerns are affected by processing are also indispensable for effective protection of self-determination with regard to information.

The DSGJZ is taking these important steps, and we are confident that this will continue to be an integral part of religious data protection in the years to come.

We are presenting our 2019 Activity Report. As usual, in addition to a summary of the development of data protection law at the European, German and religious-association levels, we also provide examples of significant events in the reporting period that may be of general importance.

Finally, our thanks go to all those who work hard to ensure that data protection is truly put into practice and who protect data and safeguard rights out of conviction.

Berlin, December 2020

Andreas Schlack
Board

1

Areas of Focus

1. Areas of Focus – Data protection developments in 2019

1.1 European Union

Data protection never stands still, but it evolves and adapts to the needs of data holders. Thus, an evaluation of the GDPR from the perspective of the European Union is planned for May 2020, since the GDPR must be evaluated and reviewed on a regular basis (cf. Article 97(1) GDPR). Further evaluations must be conducted every four years thereafter.

In the course of an evaluation, the European Commission must submit a report to the European Parliament and the Council, which must also be published and made available for viewing. If necessary, the Commission will submit proposals to amend the GDPR on this basis. Regular exchanges between the European Commission and the Member States must be conducted in Brussels beforehand.

The evaluation is also relevant to the religious association **Jehovas Zeugen in Deutschland, K.d.ö.R.** Even though the GDPR does not apply to the field of religious activity directly, Article 91 GDPR nevertheless constitutes a key provision that sets the level of data protection in the GDPR as a benchmark that must also be met by the religion's own law. The two sets of rules must correspond in all essential respects.

It is not necessary to have an exactly similar piece of legislation, but one that complies with the main contents and principles of the GDPR in the specific circumstances of ecclesiastical data processing.

It remains to be seen in the upcoming 2020 Activity Report whether and, if so, what adjustments are to be made by the European Union and what impact this will also have on the ecclesiastical data protection of the DSGJZ.

1.2 EU-U.S. Privacy Shield

In order to replace the International Safe Harbour Privacy Principles annulled by the European Court of Justice (Judgment of 6 October 2015, "*Schrems I",* C-362/14, EU:C:2015:650), the EU negotiated a treaty with the United States regarding the exchange of data between institutions and companies in both trade zones. The treaty is known as the EU-U.S. Privacy Shield.

As part of this agreement, the Privacy Shield must be reviewed annually to ensure the level of data protection to secure personal data continues to match the EU level and is not undermined. In general, this review by the European Commission in October 2019 found that the United States ensures an adequate level of protection for personal data.

We await the CJEU decision (in the pending Case "*Schrems II",* C-311/18) on the judicial review of the compatibility of the handling of personal data in the United States according to data protection law.[1]

1.3 Changes in German data protection law

On 20 November 2019, the Bundestag issued the Second Act on Amending the Data Protection Act to the provisions of the GDPR (BGBl. I., p. 1626). In 155 provisions, numerous – but no serious – amendments were made to individual laws in order that they align with the GDPR. In most cases, these were formal amendments that were already overdue.

[1] Following the period covered by the 2019 Activity Report, the CJEU issued a judgment and declared the EU-U.S. Privacy Shield invalid. The 2020 Activity Report will consider this ruling in depth.

1.4 ePrivacy Regulation

It was basically planned to have a Regulation on electronic communications enter into force simultaneously with the GDPR (ePrivacy Regulation: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC).

This Regulation would codify rules to regulate the use of electronic communications with the goal of ensuring comparable competitive conditions for all market participants. Originally, after numerous delays, the ePrivacy Regulation was set to be adopted after the European Parliament elections in 2019.

However, there were further delays, since the EU Member States were not able to reach an agreement on the draft text of the Regulation in the Council. Following the failed negotiations, as well as a transitional period of 24 months set out in the ePrivacy Regulation, any new legislation is not expected to enter into force at least before 2023.

Our Supervisory Authority continues to follow the process with great interest, even though it is currently impossible to say exactly when a new proposal can be expected. The process will be monitored further in the next activity report. Should a draft be available by then, it will be considered in view of its data protection relevance for religious data protection.

1.5 German Federal Data Protection Act (BDSG)

In April 2017, the German Bundestag passed the German Federal Data Protection Act (new BDSG) as Article 1 DSAnpUG-EU (Act on Amending Data Protection to Align with Regulation (EU) 2016/679 and Implementing Directive (EU) 2016/680). The new German Federal Data Protection Act entered into force simultaneously with the GDPR.

One provision in the German Federal Data Protection Act is also of particular importance to religious data protection supervisory authorities. The provision in § 18(1) BDSG (new) reads as follows:

> "The Federal Commissioner and the supervisory authorities of the Länder[2] (supervisory authorities of the Federation and the Länder) shall work together in European Union matters with the aim of consistently applying Regulation (EU) 2016/679 and Directive (EU) 2016/680. Before submitting a common position to the supervisory authorities of the other Member States, the European Commission or the European Data Protection Board, the supervisory authorities of the Federation and the Länder shall give each other the opportunity to comment at an early stage. For this purpose, they shall share all relevant information. The supervisory authorities of the Federation and the Länder shall consult the specific supervisory authorities established under Articles 85 **and 91** of Regulation (EU) 2016/679 if these authorities are affected by the matter." (Emphasis added.)

The consistency mechanism provided for in both the GDPR and the BDSG is always necessary when numerous supervisory authorities are involved. This may be the situation when the case facts cross different boundaries or whenever the processing of a data protection request affects the jurisdiction of several authorities. These are then obliged to cooperate with each other and, if necessary, with the Commission for the purpose of a uniform application of the GDPR.

Section 18(1), sentence 4 BDSG (new) now states that the supervisory authorities of the Federation and the Länder must consult the specific supervisory authorities established under Articles 85 and 91 GDPR if these authorities are affected by the matter. This also serves the objective of a uniform application of the GDPR and thus also of the religion's own data protection rules, such as the DSGJZ.

Even though this obligation to involve the ecclesiastical data protection supervisory authorities does not yet appear to have been fully implemented at the national level, it does constitute current national law. Therefore, we must wait and see how the churches will be perceived and how they will be able to participate actively in the consultation process independently.

[2] Translator's note: *Länder* refers to the 16 partly sovereign states within Germany.

1.6 Data Protection Act of Jehovah's Witnesses

Shortly after being awarded corporation rights, the religious association issued its own Data Protection Act that entered into force on 13 February 2008, and the new version on 1 April 2011, and guaranteed religious adherents and all others that their data would be handled in a trustworthy and at the same time secure manner. On 21 May 2018, a new version of DSGJZ was published, which came into force on 24 May 2018.

Article 91 GDPR guarantees that churches can continue to apply their own data protection rules after the GDPR comes into effect on the condition that "[w]here … churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing". The religious association of *Jehovas Zeugen in Deutschland K.d.ö.R.* complied with this condition in the form of the DSGJZ.

According to § 1(1) DSGJZ, the purpose of the DSGJZ is to protect individuals from having their privacy violated by the processing of personal data, while at the same time enabling the secure and free flow of such data.

This purpose is secured primarily by granting rights. The DJGJZ establishes the right to transparency and the right to access information, the right to rectification, the right to erasure ("right to be forgotten"), the right to restriction of processing, the right to data portability, as well as the right to file objections and complaints with the Data Protection Supervisory Authority.

(1) Rights to Transparency and to Access Information
In order for a member of the religious association or a third party to exercise his/its own rights, it is essential to know what personal data are being stored and processed. In order to meet this need – in this increasingly digital world – the DSGJZ laid down the duty to have transparent information in § 7 and § 8. In this respect, the DSGJZ is based on the standard that has been established throughout Europe by the GDPR. In addition, according to § 9 DSGJZ, every data subject has the right to access information about his data.

(2) Right to Rectification
Since there is no justification for processing incorrect data, it is essential to make provision for the rectification of erroneous data. This right is ensured under § 10 DSGJZ. However, the DSGJZ also strikes a balance between the credibility of the existing data and the interest of

each data subject. Thus, the incorrectness of the data is a prerequisite for its rectification. The data subject must therefore explain the extent to which the data is incorrect.[3]

(3) Right to Erasure

When certain grounds listed in the DSGJZ are indicated, the data subject has the right to demand the erasure of his personal data in accordance with § 11 DSGJZ. This is particularly the case if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or if consent is withdrawn and there are no overriding legitimate grounds for the processing.

(4) Right to Restriction of Processing

When disputes arise regarding the lawfulness of the processing of personal data, but erasure is not possible for reasons stated in the law, the data subject can, under certain circumstances, have the processing of his data restricted (§ 12 DSGJZ). This provides additional protection for all data subjects and prevents data – apart from their being stored – from being further processed.

(5) Right to Data Portability

Newly introduced into the DSGJZ, under § 14 DSGJZ, in line with the GDPR standard is the right to data portability – the right to obtain, under certain conditions, a copy of one's own data in a common and machine-readable file format. This should enable the data subject to transmit his data to another data controller.

(6) Right to Object

In general, the DSGJZ grants data subjects the right to object to the processing of their personal data in § 15 DSGJZ. In accordance with § 15(3) DSGJZ, the data subject must be notified of this right by the time of the first communication at the latest.

(7) Right to Lodge Complaints

The DSGJZ naturally grants legal protection to data subjects. Any data subject can contact a data controller and assert his rights. If the data subject believes that his rights have been violated, he has the right to lodge a complaint with the Data Protection Supervisory Authority in accordance with § 26 DSGJZ, which in turn monitors that data controllers comply with all data protection laws.

[3] Cf. Stade Administrative Court, decision of 9 October 2018 – 1 B 1918/18.

The DSGJZ thus has a variety of both familiar and new options for every data subject to ensure confidential and lawful handling of their personal data. In particular, due to the typical closeness between a religious association and its members, the processing of personal data is carried out in accordance with the data-protection principles in § 3(1) DSGJZ of lawfulness, of processing in accordance with fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality.

Seven Principles

- Lawfulness, principle of fairness, comprehensibility [*Art. 5 GDPR, § 3(1) DSGJZ*]
- Purpose limitation [*Art. 5(1)(b) GDPR, § 3(1) DSGJZ*]
- Data minimisation [*Art. 5(1)(c) GDPR, § 3(1) DSGJZ*]
- Integrity and confidentiality [*Arts. 32, 5(1)(f) GDPR, § 3(1) DSGJZ*]
- Storage limitation [*Art. 5(1)(e) GDPR, § 3(1) DSGJZ*]
- Accuracy [*Art. 5(1)(d) GDPR, § 3(1) DSGJZ*]
- Accountability [*Art. 5(2) GDPR, § 3(2) DSGJZ*]

Reasons for Processing

- Consent [*Art. 6(1)(a) GDPR, § 4(1)(2) DSGJZ*]
- Contract [*Art. 6(1)(b) GDPR, § 4(1)(3) DSGJZ*]
- Legal obligation [*Art. 6(1)(c) GDPR, § 4(1)(4) DSGJZ*]
- Vital interests [*Art. 6(1)(d) GDPR, § 4(1)(5) DSGJZ*]
- Tasks in the public interest [*Art. 6(1)(e) GDPR, § 4(1)(6) DSGJZ*]
- Legitimate interests of data controllers [*Art. 6(1)(f) GDPR, § 4(1)(7) DSGJZ*]
- Other reasons for processing [*Art. 4(1)(1) DSGJZ*]

Individual Rights

- Information [*Art. 12 GDPR, § 8 DSGJZ*]
- Obligation to notify data subject [*Art. 19 GDPR, § 13 DSGJZ*]
- Right to access [*Art. 15 GDPR, § 9 DSGJZ*]
- Right to rectification [*Art. 16 GDPR, § 10 DSGJZ*]
- Right to erasure [*Art. 17 GDPR, § 11 DSGJZ*]
- Right to restriction of processing [*Art. 18 GDPR, § 12 DSGJZ*]
- Right to data portability [*Art. 20 GDPR, § 14 DSGJZ*]
- Right to object [*Art. 21 GDPR, § 15 DSGJZ*]

In order to avoid regulatory gaps, the DSGJZ places particular value on maintaining the level of protection of the GDPR and implementing its basic concepts. Hence, § 1(6) DSGJZ establishes that the DSGJZ must be interpreted in a way that maintains the level of protection in the GDPR. As a result, § 1(7) DSGJZ establishes that, where necessary, the GDPR regulations and the data protection laws of the state – in this case, the German Federal Data Protection Act in particular – will be applied mutatis mutandis as part of the GDPR.

In this sense, the religious association has sought and achieved harmonisation with the GDPR beyond what is mandatory.

2

Data Protection under Ecclesiastical Law

2. Data Protection under Ecclesiastical Law

2.1 Data Protection Supervisory Authority of Jehovah's Witnesses

The Data Protection Supervisory Authority of Jehovah's Witnesses must fulfil the conditions laid down in Chapter VI of the GDPR (Art. 91(2) GDPR, Art. 51 to Art. 59 GDPR) and the religious association Jehovas Zeugen in Deutschland K.d.ö.R. has implemented this by means of § 23 to § 29 DSGJZ.

Consequently, the Data Protection Supervisory Authority of Jehovah's Witnesses was founded on 24 May 2018 and appointed as a supervisory authority over the processing operations of the religious association in accordance with the DSGJZ.

The competence of the Data Protection Supervisory Authority stems from § 24(1) DSGJZ, which states that it monitors compliance with the DSGJZ and other data protection laws. According to § 24(2) DSGJZ, the Data Protection Supervisory Authority conducts this activity over all structural divisions and agencies of the religious association (§ 5(1)(2) StRG).

The principle objective of the Data Protection Supervisory Authority is to ensure compliance with the DSGJZ in comparability with the GDPR and to ensure that the activities of the aforementioned structural divisions and agencies are compatible with data protection standards.

The competence of the Data Protection Supervisory Authority also extends to structural divisions of the worldwide religious association in other countries insofar as these are responsible for data processing in Germany. For example, this is the case with *Jehovas Zeugen in Österreich* (JZÖ). Finally, third parties outside the religious association are also covered by the supervision of the Data Protection Supervisory Authority insofar as they cooperate with the religious association.

2.2 Current developments

When it comes to data protection in practice, inquiries in line with Article 15 GDPR – the right to obtain information about the processing of personal data – play a major role. As great as the interest in the right to access information is, the questions linked to this right are also complex. In 2019, decisions, primarily from labour courts, led to a differentiation being drawn between some of the issues relating to 'information and copies'.

According to Article 15(3), sentence 1 GDPR, "the [data] controller shall provide a copy of the personal data undergoing processing." The scope of this 'right to obtain a copy' was the bone of contention in a high-profile decision before the Regional Labour Court of Baden-Württemberg (Regional Labour Court of Baden-Württemberg, *ZD* 2019, p. 276, with comments from T. Wybitul; the appeal is pending in the Regional Labour Court of Baden-Württemberg, case no. 5 AZR 66/19) and continues to be heavily disputed. Both a narrow and a broad interpretation of the 'right to obtain a copy' are advocated (for more on the dispute, see Wybitul/Brams, *NZA* 2019, p. 672).

Surprisingly, in the aforementioned judgment, the judges largely left it open as to exactly what should be copied and made available. In particular, the Court made no determinations as to whether the data controller must also provide system extracts with raw data and exported files from individual applications. In addition, it remains open whether the data subject must also disclose email correspondence that is related to the services or conduct of the plaintiff. The Court does not go into detail as to precisely which data the data controller should disclose. This is not only problematic from a legal point of view with regard to the necessary legal certainty. The decidedly vague decision leaves data controllers in the dark when it comes to how they should deal with requests for information in the future.

Article 15 GDPR regulates the right to access information and the right to obtain a copy in a clear legal structure, which speaks against the broad interpretation of the rule that was assumed by the Regional Labour Court of Baden-Württemberg. According to Article 15(3), sentence 1 GDPR, "[t]he [data] controller shall provide a copy of the personal data **undergoing processing**."

As already explained, there are different views on how far the right to obtain a copy should extend.

a) Broad interpretation

Some authors argue – regardless of practical difficulties – that data controllers must provide data subjects with all their personal data in the form of copies (cf. Kremer, *CR* 2018, p. 560 (563f.); Franck in Gola, *DS-GVO*, 2nd ed., 2018, Art. 15, par. 28).

Article 15(3) GDPR must therefore be understood to mean that the data controller must disclose all raw data. The proponents of this broad concept explain their interpretation in terms of the statutory arrangement, among other things. This suggests that the right to obtain a copy should stand alongside the general right to obtain the information listed under Article 15(1) GDPR. The right to obtain copies is therefore not limited to the information listed under Article 15(1) GDPR.

b) Narrow interpretation

This is countered by the argument that the right to obtain a copy regulated in Article 15 (3) GDPR is merely an auxiliary claim to the right to access information in Article 15(1) GDPR (cf. Dausend, *ZD* 2019, p. 103 (106f.); Dzida, *BB* 2018, p. 2677 (2679f.); Paal in Paal/Pauly, *DS-GVO BDSG,* 2nd ed., 2018, DS-GVO Art. 15, par. 33; Wybitul/Neu/Strauch, *ZD* 2018, p. 202 (203)). Therefore, the substantive scope of the right to obtain a copy does not extend beyond the compulsory information regulated in Article 15(1) GDPR (Paal in Paal/Pauly, *DS-GVO,* Art. 15, par. 33; Kamlah in Plath, *DS-GVO/BDSG,* 3rd ed., 2018, Art. 15, par. 16; cf. the statement from Bavaria State Office for Data Protection in Activity Report 8 (2017/2018), 46f.) Accordingly, data subjects may only request a copy of the information regulated in Article 15(1)(a)-(h) GDPR.

c) Statements from Data Protection Supervisory Authorities

The relevant short paper from the German Data Protection Conference regarding the right to access information in accordance with Article 15 GDPR provides no clarification on this issue. Individual statements from German data protection supervisory authorities suggest that they also tend toward the approach advocated here and generally wish to interpret the right to obtain a copy less broadly in practice. Meanwhile, the Bavaria State Office for Data Protection officially confirmed this narrow viewpoint in its 2017/2018 Activity Report, according to which Article 15 GDPR does not justify a general right to obtain copies of documents or files (cf. 2017/2018 Activity Report, Bavaria State Office for Data Protection, 22 March 2019, 46f.). The wording of Article 15(3) GDPR does not allow for the conclusion that data controllers must provide copies of files or other documents (Wybitul/Brams, "Welche Reichweite hat das Recht auf Auskunft und auf eine Kopie nach Art. 15 I DS-GVO?", (*NZA* 2019, p. 672).

A consideration of the case law of the CJEU and German courts likewise creates the impression that the right to obtain a copy should be interpreted narrowly.

In a 2014 decision regarding the Data Protection Directive (Directive 95/46/EC), the CJEU stated that the primary purpose of the right to access information is to enable data subjects to review the data processing activities that affect them (*NVwZ-RR* 2014, 736 = *ZD* 2014, 515, par. 57 – Judgment of 17 July 2014, *YS and Others,* C-141/12, EU:C:2014:2081, para. 57. In its reasons for the decision, the CJEU referred to the guarantees in Article 12 of Directive 95/46 and Article 8(2) of the Charter). Therefore, it is sufficient for a data controller to provide a data subject with a complete overview of his data in an understandable form. Accordingly, the data subject does not have the right to receive complete copies of all documents containing his personal data (paras. 58-60 of the Judgment in *YS and Others*).

Although the CJEU is referring to the previous Directive 95/46/EC, the legal evaluation can nevertheless be transferred to the current legal situation. Just like Article 15 GDPR, the Directive 95/46/EC provided data subjects with the right to inspect documents/records. It is reasonable to conclude that the EU legislator intended to anchor a right to inspect documents/records in Article 15(3) GDPR that would align with Article 12 Directive 95/46/EC. Thus, the CJEU decision can also be applied to the interpretation of Article 15(3) GDPR (as the opinion of the Bavaria State Office for Data Protection does).

In more recent decisions, Cologne Higher Regional Court and Dortmund Administrative Court Dortmund (cf. Cologne Higher Regional Court, *ZD* 2018, p. 536 = BeckRS 2018, 17378 [No. I 4]; Dortmund Administrative Court, *NJOZ* 2018, 1420 = *ZD* 2018, p. 38) have expressly adopted the approach advocated by the CJEU for the German law applicable to date. The specific issue therein was how far the right to access information in § 34 of the former version of the BDSG extends.

d) A decision by Hesse Regional Labour Court is also noteworthy (cf. Hesse Regional Labour Court, *ZD* 2013, 413 = BeckRS 2013, 67364). It made clear that employees should not be able to assert their right to access information “in the absence of sufficient facts”. Rather, it must be clear which data the request for information relates to.Summary

As a supervisory authority, the Data Protection Supervisory Authority of Jehovah’s Witnesses takes an approach that aligns with the meaning and purpose of the right to access information and the related right to receive copies of the data.

It is necessary for the data controller to comply with the right of the data subject. On the other hand, the right to access information and receive copies of personal data does not result in a full right to inspect records/files or obtain a copy of the document or the original file in which those data appear.

We now wait to see how the appeal admitted against the decision of Regional Labour Court of Baden-Württemberg will assess the matter and whether a subsequent decision will follow under EU law. In the meantime, it is preferable to coordinate the process of issuing information pursuant to § 9 DSGJZ with the Data Protection Supervisory Authority.

2.3 Cooperating with supervisory authorities of the state

The Data Protection Supervisory Authority of Jehovah's Witnesses seeks to foster cooperation and encourage exchange with the supervisory authorities of the state. In particular, this cooperation, which is standardised for state supervisory authorities in Article 57(1)(g) GDPR, should ensure that, on the one hand, the high level of data protection is maintained and, on the other hand, no isolated solutions are created that could result in data subjects receiving unequal treatment.

This cooperation could be continued during the period covered by this report.

3

Facts and Figures

3 Data protection operations during the reporting period

3.1 Statistics

In a working group, the data protection supervisory authorities of the state put forward proposals to standardise activity reports. The Data Protection Supervisory Authority of Jehovah's Witnesses did not participate therein, nevertheless, this report builds on the good results of this working group as it evaluates operations over the past year. This has also been done to facilitate comparisons between reports.

The working group proposed that the statistical section should be entitled "Facts and Figures". Subsections, such as "Complaints", "Data Protection Breaches", etc., should also be consistently used and listed. The Data Protection Supervisory Authority of Jehovah's Witnesses also follows these proposals of the working group.

Complaints:

For this section, the working group proposed the following:

> *"This section provides an overview of the number of complaints received during the reporting period. Instances received in writing, in which a natural person states that he is personally affected, are counted as complaints."*

In the following, a distinction is made between submissions from complainants whose own rights may have been violated by the facts presented (= **complaint**) and those for whom this is not the case (= **review request**). This distinction is of vital importance in view of § 27(1) sentence 2 DSGJZ. Only in cases of complaint does the three-month deadline laid down in § 27 DSGJZ apply for the Data protection Supervisory Authority. When a review is solely requested, on the other hand, the Supervisory Authority is under no obligation to respond within a specified period of time. The requesting party is merely informed that his message was received.

The complaints (meaning possible breaches of the data subjects' own rights) that were filed were processed by the Data Protection Supervisory Authority. The Data Protection Supervisory Authority usually receives complaints by post or email. Due to the sensitivity of data protection matters, the Data Protection Supervisory Authority must insist on obtaining proof of identification from a data subject before processing his concerns. This should ensure that no personal data is passed on to unauthorised third parties. Even if this procedure prolongs the processing of a data subject's requests, the Data Protection Supervisory Authority considers it indispensable to ensure that only authorised persons have access to data at any given time.

During the reporting period, all complaints and review requests submitted to the Data Protection Supervisory Authority were processed.

In five cases, the complaints were settled by agreement. In another four cases, the work of the Data Protection Supervisory Authority resulted in the partial remedy of complaints (partial erasure or rectification by the data controller).

In summary, it can be said that all proceedings before the Data Protection Supervisory Authority could be terminated by decisions or amicable settlements.

In the remaining cases of review requests, no legal infringements were found or they could not be attributed to any person.

Consultations/Advice:

For this section (with slight adjustments), the aforementioned working group made the following suggestion:

> *"Here is an overview of the number of consultations. This summarily includes consultations with data controllers, data subjects, and the religious association."*

According to § 24(3) DSGJZ, the core responsibilities of the Data Protection Supervisory Authority include to provide advice and promote awareness of data protection issues. For this reason, written and (remote) verbal consultations are held on a regular basis to prevent data protection breaches.

This instrument can be used in advance to prevent data protection from being insufficiently implemented during processing operations. For this reason, there were a large number of consultations during the reporting period. Amongst other things, the data controller was advised on the application of the Data Protection Act of Jehovah's Witnesses (DSGJZ). Furthermore, the Data Protection Supervisory Authority also acted when contracts to process orders were drawn up between the agencies of the religious association. In this way, it was possible to ensure from the very beginning that the standards of the DSGJZ, and thus also those of the GDPR, were taken into account.

Finally, adjustments to data security were achieved by means of consultations. This also included procedures under ecclesiastical law. In the processing of video recordings in particular, the religious association was advised on how to minimise data.

Data breaches:

For this section, the aforementioned working group made the following suggestion:

> *"Here is an overview of the number of written reports on data breaches received from the data controller."*

This involves recording the "data breaches" that data controllers report to the Data Protection Supervisory Authority.

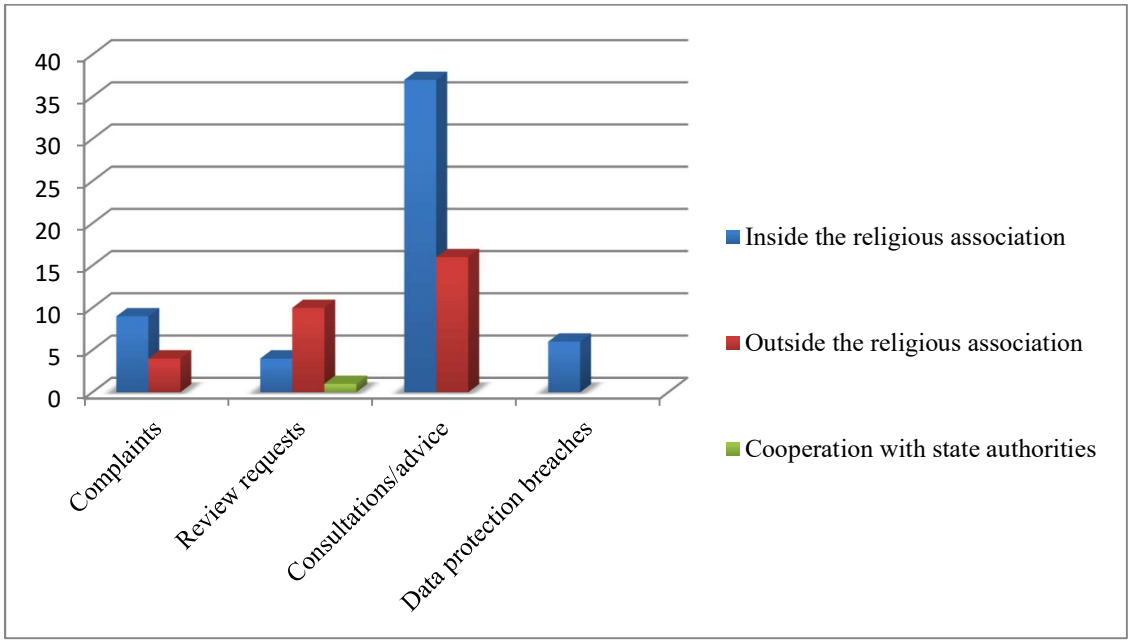
Data breaches have already been minimised through numerous security measures, even before the introduction of the DSGJZ in its current version.

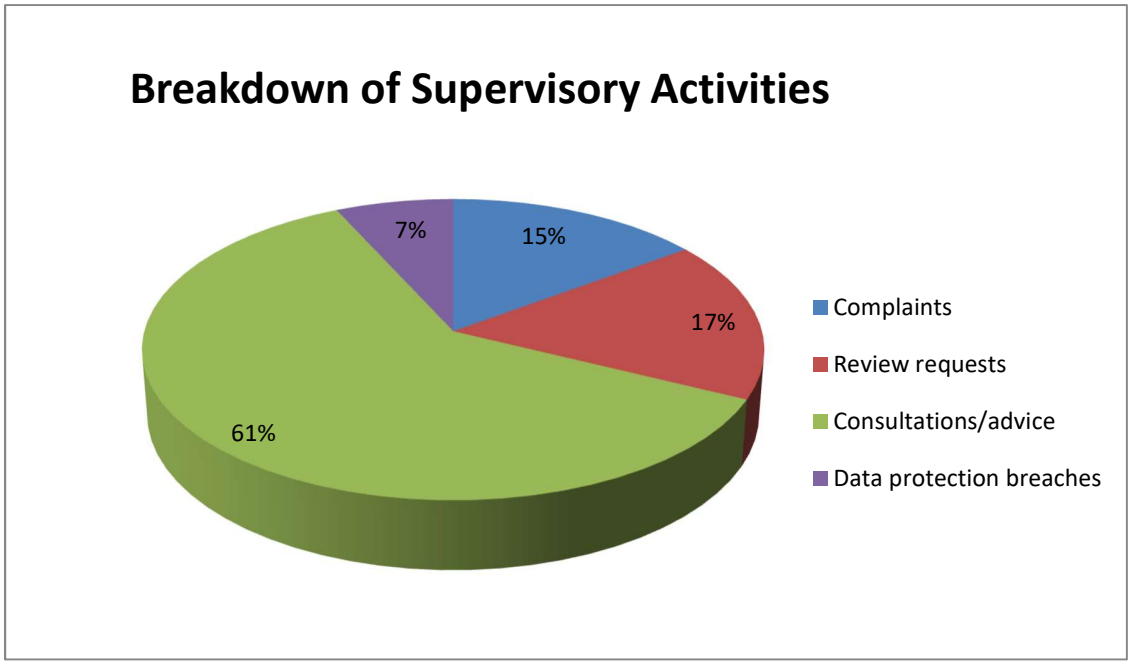
In most cases, by promoting awareness among data controllers, it is possible to comply with the 72-hour deadline pursuant to § 19 DSGJZ, Article 33(1) GDPR and to report data breaches during the reporting period.

In five reported cases of a data breach, complaints were immediately lodged for theft. The Data Protection Supervisory Authority was informed of the data breach in each case.

The Data Protection Supervisory Authority notes that the religious association manages data breaches with the necessary seriousness and takes measures to prevent the recurrence of such data breaches.

Given the above categories, a graphical analysis of the activities of the Data Protection Supervisory Authority during the reporting period is as follows:


40
35
30
25
20
15
10
5
0
Complaints
Review requests
Consultations/advice
Data protection breaches
Inside the religious association
Outside the religious association
Cooperation with state authorities


Breakdown of Supervisory Activities
7%
15%
17%
61%
Complaints
Review requests
Consultations/advice
Data protection breaches

3.2 Infrastructure

The office of Data Protection Supervisory Authority of Jehovah's Witnesses is located in Berlin at the following address:

Grünauer Straße 104, 12557 Berlin

Our office is open between 9.00 a.m. to 12.00 p.m. from Monday to Friday.

3.3 Website

The website of Data Protection Supervisory Authority of Jehovah's Witnesses can always be accessed at:

www.datenschutz-jehovaszeugen.de

The site is continually updated in line with current state of ecclesiastical as well as secular data protection law.

However, in addition to reporting in writing or by telephone, anyone who visits the website has the option of reporting his request to the Data Protection Supervisory Authority of Jehovah's Witnesses by using the online reporting form.

4. GLOSSARY

- **Data subject** — An identified or identifiable natural person to which personal data refers; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Data minimisation** — Above all, this principle states that data collection and processing must be limited to the minimum necessary for the purposes of the data processing.

- **DSGJZ** — Data Protection Act of Jehovah's Witnesses – the Data Protection Act of Jehovah's Witnesses is also a component of ecclesiastical law. This Act regulates the processing of personal data by the religious association of Jehovah's Witnesses.

- **DSGVO** — The General Data Protection Regulation (Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) of 2016 unifies the rules for the processing of personal data by companies, public authorities and associations within the European Union. The handling of data is clarified in eleven chapters with a total of 99 Articles.

- **Integrity and confidentiality** — When processing personal data, appropriate security mechanisms must be in place to prevent unauthorised and unlawful processing of personal data as well as loss or damage.

- **Consistency mechanism** — The consistency mechanism is regulated in Article 63 GDPR. This means that supervisory authorities must cooperate with each other (horizontally) and, where relevant, with the Commission (vertically) in order to contribute to the consistent application of the GDPR. This is especially the case between the lead supervisory authority and the other supervisory authorities concerned. In this respect, this norm complements the general provisions on cooperation between supervisory authorities (Article 60ff. GDPR). Such cooperation should uniformly impact not only legislation through the GDPR in all

	Member States, but also enforcement by supervisory authorities. Additionally, the newly established European Data Protection Board (Article 68 GDPR) should play a central role in the consistency mechanism.
• Personal data	Personal data are individual details about personal or factual circumstances of a specific or identifiable natural person (data subject).
• Ecclesiastical law	The law drawn up by the religious association (itself) in order to organise and manage its own affairs (for example, the statutes of the religious association).
• Accuracy	Personal data must be factually accurate and kept up to date. Inaccurate data must be erased or rectified.
• Storage limitation	This principle complements purpose limitation. The data may be stored as long as is necessary to achieve the purpose pursued by the data processing.
• Fairness/transparency	Personal data processed lawfully, in accordance with the principle of fairness and in a transparent manner in relation to the data subject. In particular, these principles are specified in concrete terms by the DSGJZ obligations to provide information and notification.
• Purpose limitation	Personal data may only be collected for specified, explicit and lawful purposes.