DATA PROTECTION SUPERVISORY AUTHORITY OF JEHOVAH'S WITNESSES

2021 Activity Report

2021 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) DSGJZ). This report covers the period from January 2021 to December 2021.

The annual report can be viewed on our website:
https://datenschutz-jehovaszeugen.de/en/download-en/

LEGAL NOTICE

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 March 2023

Content

NOTE:

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

Index of Abbreviations

BDSG	German Federal Data Protection Act
CJEU	Court of Justice of the European Union
DSGJZ	Data Protection Act of Jehovah's Witnesses
DSK	Conference of Independent Data Protection Federal and State Commissioners
EDPB	European Data Protection Board
K. d. ö. R.	Corporation under public law
SCC	Standard Contractual Clause

Introduction

In 2021, the work of the *Data Protection Supervisory Authority of Jehovah's Witnesses* was again impacted by the COVID-19 virus.

The measures that had been introduced in the previous year (meeting via videoconferencing and preaching via letter) were continued in 2021. On the one hand, we continued to take account of our brothers' interests and their associated freedom of belief, but on the other hand, we maintained a consistently high level of data protection and—where necessary—improved it even further.

In 2021, the religious association of *Jehovas Zeugen in Deutschland, K. d. ö. R.* and its structural divisions continued their efforts to find suitable digital solutions for these purposes.

During the prior reporting period, the Court of Justice of the European Union (CJEU) published a judgment on July 16, 2020 (Case C 311/18—*Schrems II* case), that invalidated the Privacy Shield Decision (Commission Implementing Decision (EU) 2016/1250 of July 12, 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield). As regards the standard data protection clauses (standard contractual clauses), the CJEU ruled that their use may continue, but they must achieve a level of protection for personal data that aligns with that of the European Union (EU).On June 4, 2021, the European Commission adopted new standard contractual clauses by means of Decision 2021/914/EU and made them available to all users through (EU) 2021/914.[1] Article 4 of the Decision requires that all "prior" standard data protection clauses be converted by December 27, 2022.

The rights of data subjects granted by the DSGJZ also provided effective protection for the personal data of data subjects in the 2021 reporting period. Both the fact that subjective rights result from these bases for claims, as well as the ever-growing interest in data protection and the ever-increasing sensitivity to it, make the DSGJZ an effective Act to protect personal data. The good experiences in 2020 were repeated in 2021.

The history of Jehovah's Witnesses in the twentieth century dramatically illustrates that the protection of personal data is not a gesture, but has been established practice for decades, precisely to ensure the protection of believers, and of third parties too.

[1] EUR-Lex - 32021D0914 - EN - EUR-Lex (europa.eu).

Preamble (2) DSGJZ

It therefore comes as no surprise that the interest in data protection issues remains high. The *Data Protection Supervisory Authority of Jehovah's Witnesses* again undertook a variety of advisory tasks and remained available in an advisory capacity for the religious association, its members, and third parties. In 2021, there were a large number of enquiries about letter witnessing, which the *Data Protection Supervisory Authority of Jehovah's Witnesses* was able to answer.

Data protection remains an issue that affects us all. It can only be implemented effectively when there exists a general awareness of data protection and a perception of its legal standards. The *Data Protection Supervisory Authority of Jehovah's Witnesses* again pursued these objectives in 2021.

One of the tasks of the *Data Protection Supervisory Authority of Jehovah's Witnesses* is to strengthen data protection as an effective instrument for trustworthy dealings. This gives all involved the opportunity to treat each other fairly and transparently while simultaneously maintaining pastoral confidentiality when necessary. This also needs to work in the digital world, but entails new risks that must be weighed carefully.

Data protection is not carried out by a supervisory authority, but primarily through the understanding and acceptance of each individual data controller and processor. Data protection thus begins with the data subject, who knows and exercises his rights. In order to effectively protect self-determination as respects information, it is imperative to understand and sense that data protection issues are affected by processing.

The DSGJZ is an effective tool to reach these high standards. This was again clearly demonstrated during the reporting period.

We now present our Activity Report for 2021. In addition to providing a summary of data protection developments at the European, national and religious community level, which has now become customary, we will also evaluate a significant decision from the Data Protection Supervisory Authority of Austria and consider its bearing on religious data protection.

Even though numerous developments and important judgments on general data protection have been made during the reporting period, please note that this Activity Report concentrates mainly on those areas which explicitly concern the religious association, or essential aspects of religious data protection.

Therefore, please see the activity reports of state data protection supervisory authorities on the development of general data protection.

Finally, our thanks go to those who work hard to apply data protection and to guarantee the rights of data subjects, striving to apply the special circumstances of religious data protection.

Berlin, March 2023

Andreas Schlack
Board

1. Area of Focus

1.1 European Union

As with the standardization of national data protection law, technical developments also set the pace for data protection law in the European Union. Global networking and the Internet are not bound by national borders and make international regulation of data protection law necessary (Taeger/Gabel/Schmidt, 4th ed. 2022, *DSGVO,* "Vorbemerkung zu Artikel 1", par. 8).

In its judgment of July 16, 2020, the CJEU declared that the Privacy Shield regulating transatlantic data transfers had an invalid legal basis.

- Standard Contractual Clauses (SCCs)

In paragraph four of the judgment, the CJEU confirmed the validity of SCCs. Nevertheless, the judgment ignited a heated discussion among data protection supervisory authorities. The rule-of-law principle set out by the CJEU in the judgment must also be considered when applying the SCC (Article 46(1) GDPR), so that the data controller must provide "appropriate safeguards" to secure personal data during data transfers. The SCCs constitute such appropriate safeguards.

On June 4, 2021, the European Commission published the final version of the revised Standard Contractual Clauses (SCCs) in an *Amtsblatt* (Official Gazette) on June 7, 2021 (Baumgartner/Hansch/Roth: "Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten", *ZD* 2021, p. 608).

- Structure of the SCCs

The European Commission opted for a "modular approach" when structuring the SCCs. The Annexes to the SCC Decision contain a collection of 18 Clauses, from which contracting parties can select those applicable to their situations. In addition to the general Clauses that apply to all constellations and have the same contents, the individual "Modules" represent four possible constellations:

- Transfer controller to controller – "C2C" (Module One),
- Transfer controller to processor – "C2P" (Module Two),
- Transfer processor to processor – "P2P" (Module Three), as well as
- Transfer processor to controller – "P2C" (Module Four).

Section I (Clauses 1 to 7 SCC), Section II (Clause 8.1 and 11(a) SCC), Section III (Clauses 14 and 15 SCC) and Section IV (Clause 16 SCC) contain general Clauses that apply uniformly and with the same contents as all the above constellations. These provisions are always included in an SCC contract, supplemented by other provisions from the individual Modules with specific Clauses according to the constellation.

As with the previous SCCs, the Clauses are supplemented by Appendices that are part of the contract and must be individualized by the parties. The new SCCs contain three Annexes:

- **Annex I** requires parties to include a detailed description of the relevant data transfers for all Modules as well as a list of the contracting parties. The purpose and scope of the data transfer (or the processing operations on which it is based), including further processing, must be described. The storage period, or the criteria for determining it, and the frequency of transfer must also be described. Annex I must also identify the supervisory authority responsible in accordance with Clause 13 SCC.
- **Annex II** requires an overview of the technical and organizational measures (TOM) that the data importer implements to protect personal data. Measures taken by the data exporter to secure the transfer of data to the data importer should also be described, although this is not expressly required under Annex II.
- **Annex III** requires that all sub-processors—if the data exporters grant specific authorization for their involvement pursuant to Clause 9(a) Option 1 SCC—be listed for Modules Two and Three, stating their names, addresses and a description of the processing.

- SCCs—Transfer Impact Assessment (TIA)

Clauses 14 and 15 SCC contain specific regulations on what is known as a Transfer Impact Assessment (TIA) and thus on a standardized risk assessment. The European Commission is directly reacting to the *Schrems II* judgment of the CJEU. It follows from recital 3 of the SCC Decision that contracting parties can add further contractual and technical and/or organizational measures and guarantees to the SCC. The state supervisory authorities (DSK) also stress the necessity of additions.[2]

Clause 14(d) SCC lays down a new formal obligation that is not found in the GDPR. The implementation and documentation of a TIA will play a significant practical role in the future.

[2] "Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse von Prof. Stephen I. Vladeck, University of Texas School of Law"—https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf.

1.2 Changes in German data protection law due to the pandemic

Nationwide, data protection issues surrounding COVID-19 were the focus of data protectors. Digital contact-tracing apps[3] related to vaccination and testing came under their special scrutiny.

In 2021, data protection was amended with regard to German media and telecommunications (German Telemedia and Telecommunications Data Protection Act; German Telecommunications Act). In addition, all stakeholders eagerly await further modernization of data protection law in electronic communications via the ePrivacy Regulation (see 1.3).

The pandemic also sent the labor market into a state of flux and caused major changes. The new conditions require supportive data protection measures. It is hard to envisage solutions for those working from home without an appropriate data protection framework.

Data protection can also pursue special protection targets, such as youths and consumers, or the protection of personality rights[4] when digitizing patient data in the German Patient Data Protection Act.[5] However, the Federal Constitutional Court[6] did not accept a constitutional complaint directed against provisions in Book V of the German Social Security Code (SGB V) regarding digitized medical files. The German government's plan to use the tax identification number as the overarching personal identity number with the aid of the Register Modernization Act met with futile resistance from the supervisory authorities.[7] The 1976 personal identification number provided for under registration law in parallel with the German Federal Data Protection Act had failed due to constitutional concerns about unlawful citizen surveillance (Prof. Peter Gola/Christoph Klug, "Die Entwicklung des Datenschutzrechts", *NJW* 2021, 2629).

[3] On the collection of contact data, see, for example, B. BayVerfGH, *ZD* 2021, 33 and VerfGH Saarl, *ZD* 2021, 35; Dieterle *ZD* 2021, 38; also see Schrahe/Städter, *DuD* 2021, 315.
[4] *Dochow MedR* 2021, 115; also see *BfDI,* 29. TB, March 25, 2021, par. 4.2.
[5] German Act on the Protection of Electronic Patient Data in the Telematics Infrastructure (Patientendaten-Schutz-Gesetz—PDSG) *BGBl.* 2020 I 2115 with critical evaluation from BfDI, 29. TB, par. 4.2.
[6] BVerfG, *NJW* 2021, 1300.
[7] BfDI, 29. TB, par. 3.1.2 and 5.1.

1.3 ePrivacy Regulation

In addition to the GDPR, the ePrivacy Regulation (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) will in future "particularize and complement" (recital 5) the general requirements of the GDPR as regards electronic communication providers and networks.

At the same time, the ePrivacy Directive, and the Cookie Directive that supplements it, will be replaced.

In recital 6 of the proposed ePrivacy Regulation, the European Commission stated that while the "principles and main provisions" of the ePrivacy Directive "remain generally sound", the Directive has not fully kept pace with the evolution of technological and market reality. These include the entrance on the market of electronic communications services. These are based on internet access services and compete with classic telecommunication services such as the telephone and text messaging (SMS).

The scope of the proposed ePrivacy Regulation has thus been significantly broadened when compared to the previous requirements (Jandt/Steidle, *Datenschutz im Internet,* B. II. Zulässigkeit der Verarbeitung personenbezogener Daten, par. 225).

Yet the ePrivacy Regulation did not undergo further significant developed during the reporting period.

The European Data Protection Board (EDPB) summarized the current situation and identified crucial unanswered questions in Statement 03/2021 on the ePrivacy Regulation.[8]

However, after the change in the presidency of the Council of the European Union on January 1, 2021, and years of discussions about the wording of the Regulation, the Portuguese Council Presidency finally succeeded in convincing the member states of its proposal of January 5, 2021—not entirely without criticism. Meanwhile, three-way negotiations with the European Parliament have begun. These are based on the version published by the Council of Ministers of the European Union on February 10, 2021.[9]

Our supervisory authority is greatly interested in these proceedings.

[8] https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_de.pdf.
[9] https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

1.4 German Federal Data Protection Act (BDSG)

The German Federal Data Protection Act (BDSG) was also evaluated in 2021 in accordance with the GDPR.

As a basis on which to evaluate the BDSG, a survey was conducted with both public and private users of the BDSG, including data protection supervisory authorities, leading business associations and other institutions involved in data protection.

According to the results of the evaluation, the BDSG has proven overall to be appropriate, practicable and legally clear, despite various criticisms, declared the German Federal Ministry of the Interior. As a result of the evaluation, the Ministry of the Interior will examine legal amendments to certain BDSG provisions.

In June 2021, on the 45th anniversary of the BDSG, the Federal Data Protection Commissioner, Professor Kelber, emphasized the value of the fundamental right to self-determination with regard to information:

> "Over the last year in particular, we observed that data protection laws proved their worth even more during a crisis."[10]

The Federal Commissioner for Data Protection and Freedom of Information explained that the basic concept behind the BDSG has not changed, but "even when the Bundestag passed the Federal Data Protection Act on June 10, 1976, the aim was to protect citizens from the misuse of their personal data. Few members of parliament probably thought about social networks, spyware used by governments and biometric video surveillance. The challenges for the BDSG continue to grow with each year".

The national BDSG also shows that it is precisely in times of crisis that the law evolves and the value of a law needs to be gauged.

[10] https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2021/11_BDSG-45-jähriges-Jubiläum.html.

1.5 Data Protection Act of Jehovah's Witnesses (DSGJZ)

Shortly after the status of a public corporation was granted, the religious association issued its own Data Protection Act that came into force on February 13, 2008, and in its revised version on April 1, 2011, which guarantees trustworthy and safe handling of personal data to its members and all others. On May 22, 2018, a revised version of the DSGJZ was published, which has been in force since May 24, 2018.

The DSGJZ guarantees the same rights for data subjects as are laid down in the GDPR. In addition, Section 1(7) DSGJZ regulates that where necessary, the GDPR regulations will be applied mutatis mutandis as part of the DSGJZ.

The 2019 Activity Report discussed in detail individual data subject rights to do with personal data. In this respect, please refer to the 2019 report for more information.

2. Data Protection under Ecclesiastical Law

2.1 *Data Protection Supervisory Authority of Jehovah's Witnesses*

The main task of the *Data Protection Supervisory Authority of Jehovah's Witnesses* is to monitor compliance with the rules of the DSGJZ and other data protection regulations (§ 24(1) DSGJZ).

Under Section 24(3), the *Data Protection Supervisory Authority of Jehovah's Witnesses* has the following additional tasks within its scope of responsibility:

- Promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing (§ 24(3) No. 1 DSGJZ).
- Advise structural divisions and agencies of the religious association on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing (§ 24(3) No. 2 DSGJZ).
- Promote awareness among controllers and processors regarding their obligations under this Act (§ 24(3) No. 3 DSGJZ).
- Handle complaints lodged by a data subject, or by a body or organization, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period (§ 24(3) No. 5 DSGJZ). To facilitate the lodging of complaints, the Data Protection Supervisory Authority provides an online form that you can fill out directly on this page.

The Data Protection Authority has fulfilled these tasks during the reporting period. The adjusted preaching methods—Jehovah's Witnesses stopped having personal conversations door to door and began writing letters—sparked numerous queries to the *Data Protection Supervisory Authority of Jehovah's Witnesses.*

- Witnessing letters

A large number of data subjects contacted the *Data Protection Supervisory Authority of Jehovah's Witnesses,* asking why they received a personal letter from one of Jehovah's Witnesses. Although the DSGJZ does not apply to personal data processing in the context of personal religious practice (§ 1(9) DSGJZ), and hence the *Data Protection Supervisory Authority of Jehovah's Witnesses* is not responsible, it was nevertheless possible to answer the questions from data subjects in the vast majority of cases.

According to the knowledge of the *Data Protection Supervisory Authority of Jehovah's Witnesses,* Jehovah's Witnesses used public sources (for example, telephone directories) to find recipients for their personal letters.

In this way, Jehovah's Witnesses could exercise their positive religious freedom and, at the same time, could show consideration for the health of all involved. All the while, no records were kept.

- Video Communication

In other instances, the *Data Protection Supervisory Authority of Jehovah's Witnesses* received queries about videoconferencing (for example, Zoom).

At the outset of the pandemic, the religious association decided to put on pause holding in-person gatherings and instead chose to meet via videoconferencing.

There was no need for participants to create their own user accounts or provide personal data. Each participant personally decided whether to mute/unmute himself or appear on camera.

In all cases, the *Data Protection Supervisory Authority of Jehovah's Witnesses* was able to answer the questions of data subjects.

2.2 Current developments

In line with the European harmonization of data protection, the *Data Protection Supervisory Authority of Jehovah's Witnesses* also considers procedures handled by other state supervisory authorities, but that are nevertheless related to the procedures of the *Data Protection Supervisory Authority of Jehovah's Witnesses.*

Administrative Decision of the Data Protection Supervisory Authority of Austria, March 23, 2021, No. D124.2701 (2020-0.829.566) (RIS - 2020-0.829.566 - Entscheidungstext - Datenschutzbehörde (bka.gv.at))

- Introduction

The Austrian Supervisory Authority had to decide on data protection complaints in which the complainant alleged that the religious association of *Jehovas Zeugen in Österreich* (respondent) violated his rights to secrecy, access to information, erasure and objection. The complainant claimed that the respondent did not fully comply with his request for information, which he addressed to [the respondent], and also failed to respond to his request for data erasure. He also maintained that his right to restricted processing had been violated, since he objected to the announcement that he is no longer one of Jehovah's Witnesses and prohibited his data from being forwarded to the branch office.

- Decision

In its decision of March 23, 2021, the Austrian Supervisory Authority dismissed all four points of the complaint, since each of them dealt with "internal matters" of the respondent, and so the Austrian Supervisory Authority had no jurisdiction given the subject matter.

- Facts

The complaint was a former Witness of Jehovah. The complaints were directed against *Jehovas Zeugen in Österreich, K. d. ö. R.*

On the basis of Article 15 GDPR, the complainant requested information from a congregation (local subdivision) of the Austrian religious association, which he obtained.

The complainant then requested that his data be erased on the basis of Article 17 GDPR. The congregation could only partially comply with this request, which it also gave reasons for when it issued him another data disclosure.

The complainant also objected to his termination of membership being announced.

In his complaint to the Austrian Supervisory Authority, the complainant alleged that his rights to access information and erasure were violated, as were his rights to confidentiality and restricted processing.

The Austrian Supervisory Authority issued its decision in March 2021. Therein, it dismissed the complaints, stating that it did not have jurisdiction over the subject matter of the complaints.

- Legal Assessment of the Data Protection Supervisory Authority of Austria

The Austrian Supervisory Authority argued that it lacked substantive jurisdiction on all points of the complaint and therefore dismissed the complaint in its entirety.

Some of its main points in support of its decision:

In point 1 of the ruling, the Austrian Supervisory Authority first stated that the complainant had been a member of the religious association and questions about membership in a religious association fall within the "internal matters" of a religious association. Hence, the Austrian Supervisory Authority has no jurisdiction in this matter. (Page 8, 9 of the decision.)

The same was said of the complainant's assertion that his right to secrecy was violated by the announcement that he terminated his membership. According to the Austrian Supervisory Authority, this came down to the arrangement of religious services and membership issues. Both are "undoubtedly" to be regarded as "internal matters", which takes away jurisdiction from the Austrian Supervisory Authority. (Page 9 of the decision.)

Point 2 of the ruling addressed the alleged violation of the right to access information. Since the complainant was demanding that "cover letters, letters of introduction, evaluations of the 'spiritual condition' of members as well as information and about him from the congregation file, and so forth" be hand over, the Austrian Supervisory Authority referred to the European Court of Justice and recital 63 GDPR. Accordingly, he had no right to demand copies of papers, entire documents or, as in this case, cover letters, letters of introduction, etc. The disclosure of information about the stored personal data was sufficient to comply with Article 15 GDPR.

Lastly, the Austrian Supervisory Authority concluded that the complainant was demanding documents that "document the concrete form of membership status" and so "undoubtedly" constitute an internal matter over which the Austrian Supervisory Authority has no jurisdiction. (Page 10 of the decision.)

Point 3 of the ruling addressed the alleged violation of the right to data erasure. The Austrian Supervisory Authority stated that this is also an "internal matter" over which it has no jurisdiction. According to the Authority, erasing data that were processed in the context of membership is also a religious association membership issue. (Pages 10 and 11 of the decision.)

- Concluding Comments

In this decision, the Data Protection Supervisory Authority of Austria correctly balanced the right of self-determination of religious associations against the rights under data protection law. It made clear that the rights arising from data protection law do not automatically supersede other

constitutionally guaranteed rights, which, as rights with equal priority, can have the effect of limiting data protection issues. In the spirit of practical concordance, the aforementioned necessary balancing of interests should lead to the greatest possible consideration of the conflicting rights.

The Data Protection Supervisory Authority of Austria defined "internal affairs" according to the binding provisions of the European Court of Human Rights and clarified that anyone who voluntarily joins a religious association accepts the consequences that result from the religious association's right to self-determination, including from a data protection perspective.

2.3 Cooperation with supervisory authorities of the State

The *Data Protection Supervisory Authority of Jehovah's Witnesses* strives to promote cooperation and expedite the exchange of information with state supervisory authorities. Such cooperation, as laid down in Article 57(1)(g) for state supervisory authorities, shall ensure that, on the one hand, the high level of data protection is provided and, on the other hand, isolated applications do not arise that could lead to discriminatory treatment of the data subject.

3. Facts and Figures

3.1 Statistics

State Supervisory Authorities set up a task force that worked on suggestions for standardizing preparation of activity reports. The *Data Protection Supervisory Authority of Jehovah's Witnesses* was not involved in this, nevertheless this report draws on the good results of the task force in evaluating its operations in the reporting period. This provides a means of comparison with other reports.

Please see previous Activity Reports for explanations of the terms: complaints, data protection breaches, review requests, consultations.

Complaints

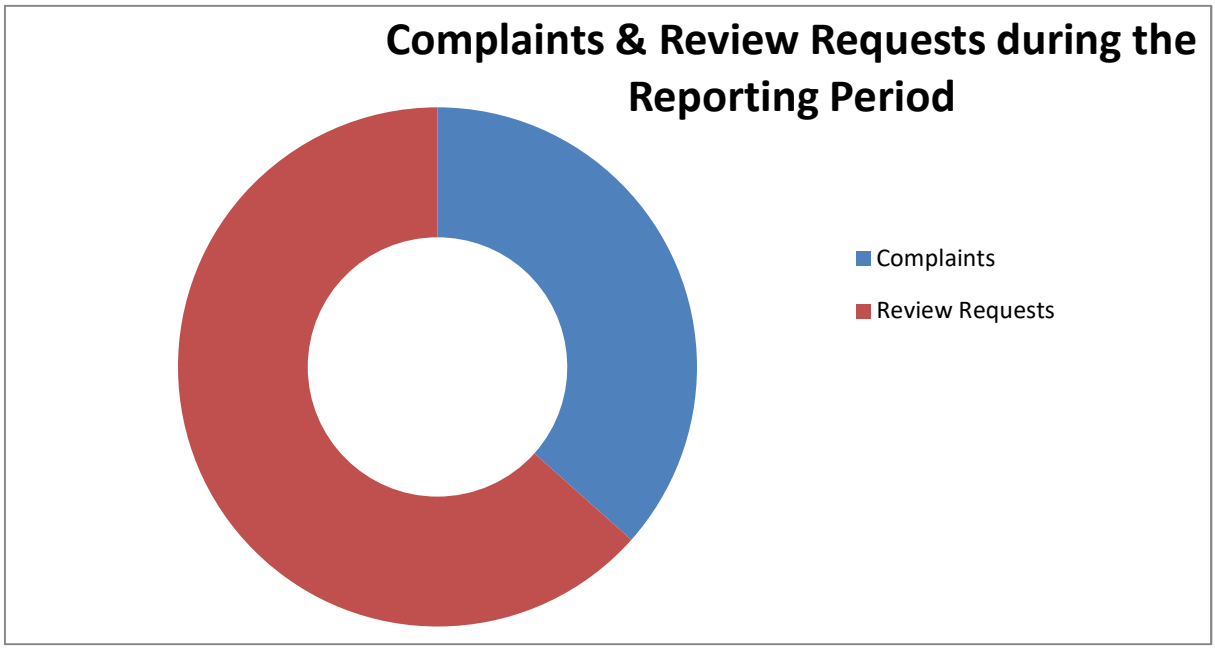
All of the complaints and review requests made to the Data Protection Authority in the reporting period could be processed.

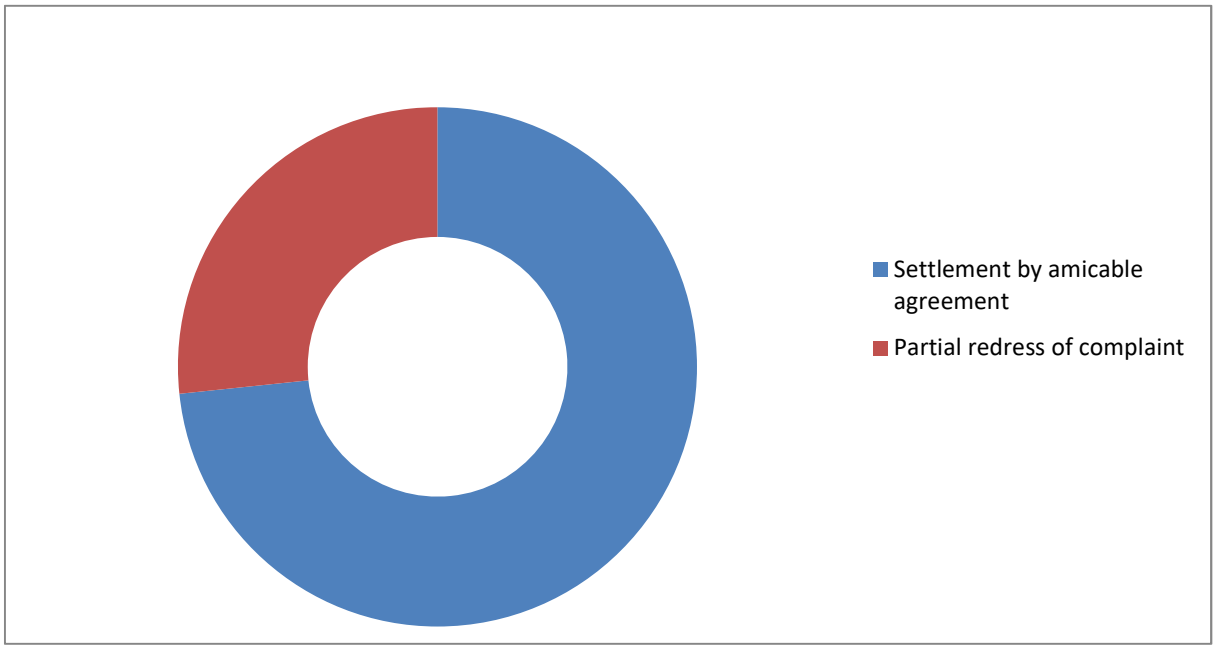
In eleven cases, the complaint was dealt with by settlement. In four other cases, the activity of the Data Protection Authority led to partial remedy of the complaint.

In summary, all proceedings brought before the Data Protection Authority could be concluded by means of a decision or by amicable settlement.

In other cases involving review requests, no infringements were apparent, or these could not be associated with a person.

The results for the reporting period are shown in the following chart:





Consultations

Under Section 24(3) DSGJZ, one of the main tasks of the data protection authority is to promote public awareness and understanding for data protection matters. For this reason, written and verbal consultations (also by telephone) take place time and again on the avoidance of data protection breaches.

By this means, it can be prevented from the start that data protection is not sufficiently observed in processing operations. For this reason, there were a number of consultations during the reporting period. The controller was advised, among other matters, regarding the application of the GDPR. The data protection authority was also involved when contracts on order processing were drawn up between facilities of the religious association. In this way it was possible to ensure from the outset that the standards of the DSGJZ, and thus also the GDPR, would be considered.

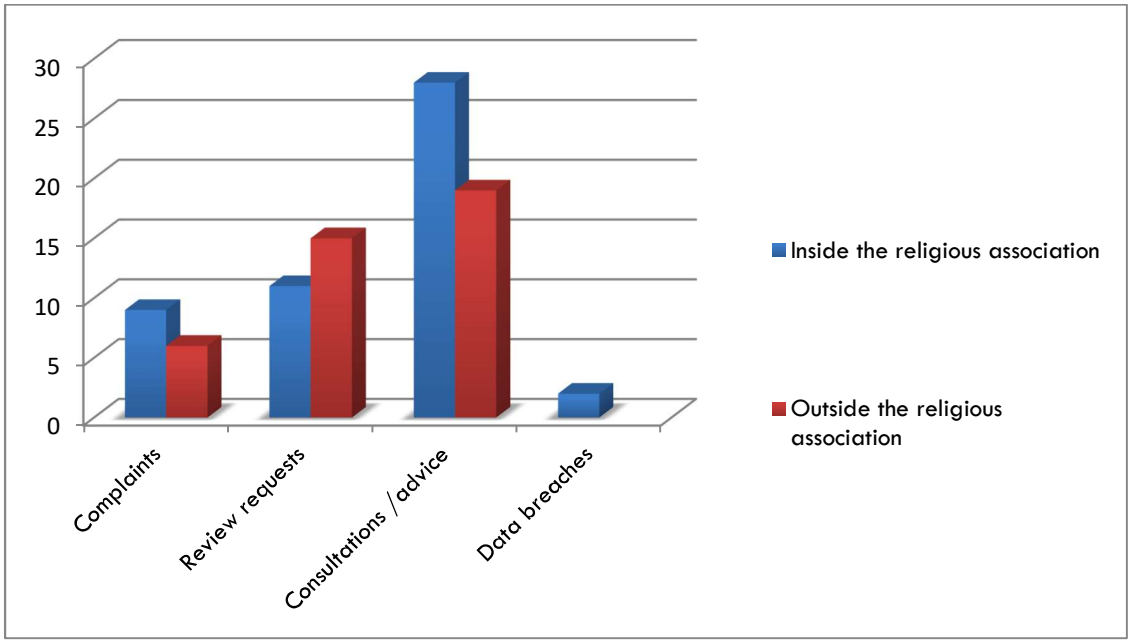
Adjustments in data security were also achieved in consultations. This included ecclesiastical proceedings.

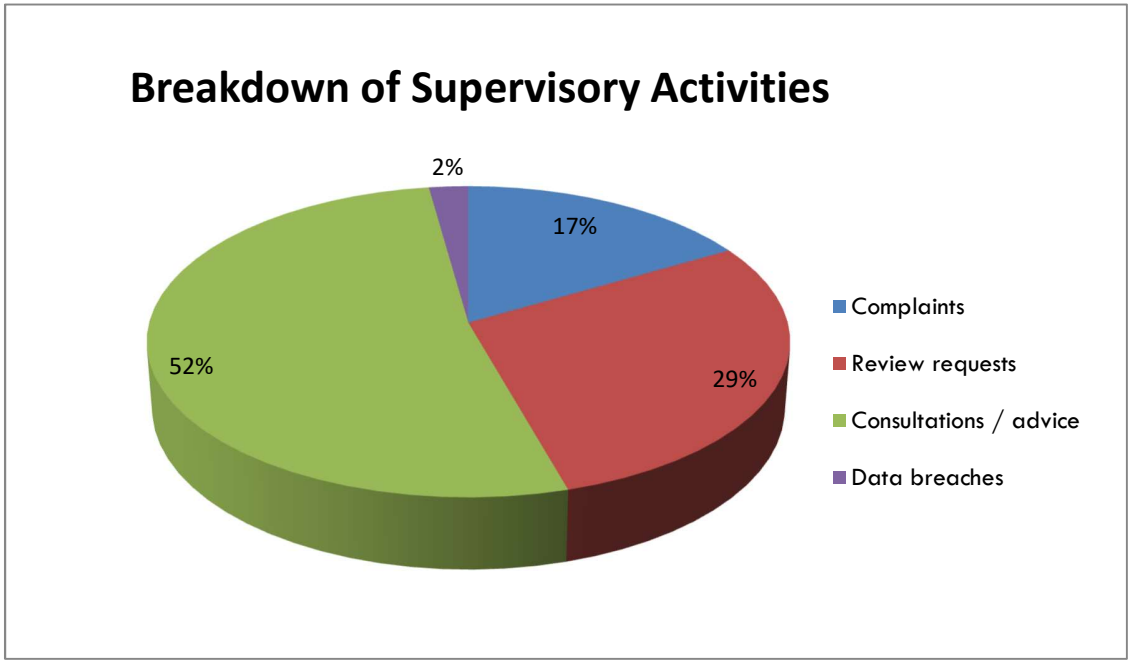
Data Breaches

In two reported cases of a data breach during the reporting period, a report for burglary was immediately filed. The Data Protection Authority was informed about each data breach.

The Data Protection Authority finds that the religious association handles data breaches with the necessary seriousness and takes measures to prevent any repetition of such data breaches.

Taking account of the above categories, the following graphic analysis shows the Data Protection Authority's activity in the reporting period:


30
25
20
15
10
5
0
Complaints
Review requests
Consultations / advice
Data breaches
Inside the religious association
Outside the religious association


Breakdown of Supervisory Activities
2%
17%
52%
29%
Complaints
Review requests
Consultations / advice
Data breaches

3.2 Infrastructure

The office of the *Data Protection Supervisory Authority of Jehovah's Witnesses* is in Berlin. The address is:

Grünauer Straße 104, 12557 Berlin

The office is open from Monday to Friday from 9:00 a.m. to 12:00 noon.

3.3 Website

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

www.datenschutz-jehovaszeugen.de

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

- 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.
- Ecclesiastical law — The law drawn up by the religious association (itself) in order to organize and manage its own affairs (for example, the statutes of the religious association).
- Personal data — Personal data are individual details about personal or factual circumstances of a specific or identifiable natural person (data subject).