

DATA PROTECTION SUPERVISORY AUTHORITY OF JEHOVAH'S WITNESSES

2020 Activity Report

2020 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 2020 to December 2020.

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 September 2021

Content

Index of Abbreviations.....	6
Introduction	7
1. Areas of Focus	10
1.1 European Union	11
1.2. EU-U.S. Privacy Shield	13
1.3 Changes in German data protection law due to the pandemic	14
1.4 ePrivacy Regulation	15
1.5 German Federal Data Protection Act (BDSG)	16
1.6 Data Protection Act of Jehovah’s Witnesses (DSGJZ)	16
2. Data Protection under Ecclesiastical Law	17
2.1 <i>Data Protection Supervisory Authority of Jehovah’s Witnesses</i>	18
2.2 Cooperation with supervisory authorities of the State	19
3. Facts and Figures	20
3.1 Statistics	21
3.1 Infrastructure	25
3.2 Website	25
4. Glossary.....	26

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 a different color in the main text (for example, **personal data**), this indicates that a more detailed explanation is available in the Glossary.

Index of Abbreviations

BCR	Binding Corporate Rules
BDSG	German Federal Data Protection Act
DSGJZ	Data Protection Act of Jehovah's Witnesses
GDPR	General Data Protection Regulation of the European Union
EDPB	European Data Protection Board
EU	European Union
CJEU	Court of Justice of the European Union
K.d.ö.R.	Corporation under public law
US	United States

Introduction

In the reporting period, the still comparatively new legal frameworks of the [DSGJZ](#) and the corresponding [DSGVO](#) had to cope with a situation that was new to everyone. The SARS-CoV-2 pandemic was, and still is, a topic affecting nearly all areas of life. It is therefore not surprising that numerous data protection issues are also linked to this topic.

Early in the pandemic, it became obvious that the customary way of life, including customary freedoms, would have to be restricted to ensure the safety of the general public. The greatest change for a religious community was having to forgo worshipping together in person. Already in March 2020, *Jehovas Zeugen in Deutschland*, K. d. ö. R. suspended in-person meetings at their Kingdom Halls and started virtual meetings using videoconferencing. Believers began to look for other ways to actively express their faith. Digitization played an important role in this. The points of contact with data protection thus become apparent.

In its statement of March 19, 2020, the European Data Protection Board (EDSA) explained that data protection regulations do not prevent taking measures against the pandemic.

A further focal point in the reporting period was the Judgment of the Court of Justice of the European Union on the invalidity of the EU-US Privacy Shield (Adequacy Decision (EU) 2016/1250 of the Commission, July 12, 2016 under Directive 95/46 of the European Parliament and the Council on the adequacy of the protection provided by the EU-US Privacy Shield) of July 16, 2020 (*Facebook Ireland and Schrems ('Schrems II')*, C-311/18, EU:C:2020:559). The 2019 Activity Report also referred to this case.

The rights of data subjects, granted by DSGJZ, form an effective framework for the enforcement of data protection claims. This again became clear in 2020. The rules, as well as the growing consciousness for data protection, are having an effect. This is especially true in proactive terms when the data protection principles under Section 3(1) DSGJZ, such as [data minimization](#), are considered from the outset and the principles of [privacy-by-default](#) and [privacy-by-design](#) are observed.

In the reporting period, interest in data protection matters continued to increase, shown by the number of consultations. The *Data Protection Supervisory Authority of Jehovah's Witnesses* is achieving its main tasks of advising [data subjects](#) and those responsible for data processing in the religious association, and raising the public's awareness for data protection matters.

Data protection will only work if all those involved in data processing are conscious of their rights and obligations and, from the start, attach importance to basic data protection standards.

Article 91 GDPR and its recital 165 continue to be relevant, serving as an interface and a bridge between the ongoing developments in the European Union's data protection law and the rules of our religious association.

The matter of confidentiality, especially due to the pastoral relationship of trust, makes it imperative for a religious association to understand data protection as an elementary component of its activity. Believers will only feel free to reveal information about themselves and their problems if a framework of confidentiality has been established (Proverbs 15:22; 25:9).

Therefore, the religious association has been making provisions in its religious law for decades to ensure that **personal data** is protected — even before data protection laws were established at the federal, federal state 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.

Data protection can no longer simply be dismissed as a tiresome activity that slows down and unnecessarily complicates work. Rather, data protection offers the possibility to cooperate with others in a fair and transparent way and, at the same time, maintain pastoral confidentiality. During the pandemic, it has been possible to successfully make the quick change to digital methods of communication, while still taking account of data protection rules and conforming with the law.

Data protection is not carried out by a supervisory authority, but primarily through the understanding and acceptance of each individual data user and processor. Data protection thus begins with the data subject. Understanding and sensing that data protection issues are affected by processing is also indispensable for the effective protection of informational self-determination.

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

We now present our Activity Report for 2020. Among others, it contains the usual summarized presentation regarding the development of data protection laws on the European, the German and the religious association levels.

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.

Berlin, August 2021

Andreas Schlack
Board

1. Areas of Focus

1.1 European Union

As noted in the previous activity report, data protection is never static, it is not an end in itself; it is there to safeguard the interests of the data subject. On June 24, 2020, in the reporting period, the European Commission published an evaluation report on the General Data Protection Regulation (GDPR) entitled **Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation** (hereafter 'evaluation report').¹

A little more than two years after the GDPR came into effect, the European Commission published its first evaluation report. According to the report, the GDPR has met most of its goals. This is mainly due to powerful and enforceable regulations for members of the public, and an innovative European governance and implementation system created under the GDPR. The GDPR proved itself to be flexible in supporting digital solutions during unexpected situations, such as the COVID-19 crisis. The report shows that harmonization is increasing in the member states, even though a certain degree of fragmentation still exists that requires constant supervision.

The report concluded that the GDPR is an overall success, with potential for further improvement. The important goals of the GDPR, including the creation of a comprehensive awareness of data protection, have been reached. Additionally, supervisory authorities have been provided with tools to better implement data protection. Worldwide, the GDPR has proved itself to be an example for new legal regulations in data protection.

In its evaluation report, the European Commission required the EDPB to intensify its work in certain areas. These include providing guidance on protective measures for data transfers to third countries, or streamlining the approval process for binding corporate rules (BCR), for example.

Such an evaluation is to be carried out every four years (cf. Article 97(1) GDPR) and is to make clear that data protection does not stand still and requires amendment.

The evaluation also involves the religious association *Jehovas Zeugen in Deutschland*, K. d. ö. R. Article 91 GDPR is a key standard that the GDPR sets as the standard level of data protection, which is also to be adhered to under ecclesiastical law. The two sets of rules are to be of equal value in all essential points.

It is noteworthy that the evaluation report does not mention religious data protection at all. At the same time, the report makes clear that a "harmonized approach" and "a European common

¹ European Union: European Commission, Communication from the Commission to the European Parliament and the Council on the Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, 24 June 2020, COM(2020) 264 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> [accessed 22 February 2022]

culture of data protection” need to be created. Of course, this basic configuration also affects religious data protection. It would be difficult to understand, and even more difficult to explain, if a data protection decision made in France had to be decided differently in Austria or Germany.

“To meet the full potential of the GDPR, it is important to create a harmonized approach and a European common culture of data protection, and to foster a more efficient and harmonized handling of cross-border cases. This is expected by people and businesses and constitutes an essential objective of the reform of EU data protection rules. It is equally important to ensure that all tools available in the GDPR are used fully to ensure an efficient application for individuals and businesses. - - When following-up on these issues, the relevant case law of national courts and the Court of Justice helps to create a consistent interpretation of data.”²

This aspect plays an important role when it comes to evaluating and, if necessary, implementing decisions made in EU Member States in connection with the religious association of Jehovah’s Witnesses for *Jehovas Zeugen in Deutschland*, K. d. ö. R. Following the main theme of the evaluation report, harmonization within the EU is to be ensured for judgments. In the light of the above, our supervisory authority examines relevant case-law of other member state courts and the Court of Justice, strives to ascertain the essence of data protection law in each case, and then to apply this in its own work.

In this way, our authority works toward harmonization in the area of religious data protection.

It is to be hoped that in the next evaluation in 2024, the EDPB gives attention to religious data protection and reinforces its role in the European context.

² Evaluation report, p. 13-14.

1.2. EU-U.S. Privacy Shield

The decision of the CJEU of July 16, 2020 was awaited with great anticipation (*Facebook Ireland and Schrems* ('*Schrems II*'), C-311/18, EU:C:2020:559). The judgment pointed out, as the decision of October 6, 2015 (*Schrems I*, C-362/14, EU:C:2015:650) already had, that transfer of personal data to a third country deserves particular attention.

In times of global data flow, data transfers seem to be unavoidable. At the same time, these must adhere to the legal framework of the GDPR. The CJEU judgment once again clarified this. With immediate effect, the CJEU declared invalid the adequacy decision for the US, the EU-US Privacy Shield. In the judgment, statements were made about transfers to the US based on the transfer mechanisms under Chapter 5 of the GDPR. The main problem seen by the CJEU were the access rights of US security agencies and the associated (nearly impossible) legal protection of data subjects in Europe. The judgment established that a sufficiently clear and precise limitation of the amount of data collected by the security agencies was lacking. In addition, basic possibilities of control by the courts is also lacking with regard to such data collection.

Section 702 of Foreign Intelligence Surveillance Act (FISA) and its PRISM program allow US security agencies to obligate service providers for electronic communication based in the US to supply all information relating to certain suspected persons. In addition, the Upstream program, which is also based on Section 702 of FISA, obligates data communicators to allow the National Security Agency (NSA) to access meta and content data for the purpose of filtering according to certain selectors.

Experts were awaiting the judgment with great interest, and its consequences are certainly immense. However, the CJEU also pointed out that data controllers can examine taking further measures that would make legal transfers possible. At the same time, the CJEU also looked into the European Union's standard contractual clauses. The existing versions are not adequate to make legal transfers possible. Nevertheless, they are an effective method that requires revision. This revision is to take place in 2021. We will therefore probably also deal with the revised standard contractual clauses in our authority's next activity report.³

³ On June 4, 2021, outside of the activity reporting period, the European Commission issued [Standard Contractual Clauses](#) that can be used for data transfers within the EU, as well as internationally.

1.3 Changes in German data protection law due to the pandemic

The corona pandemic made it necessary to put limitations on constitutionally-guaranteed civil liberties, leading to lively debate about their scope, also from the perspective of data protection⁴. The authorities faced the particular challenge of having to trace infection chains and, at the same time, adhering to data protection standards.

The discussions about the corona warning app vividly depicted the poles of opinion on this (*Engeler* NJW-aktuell Heft 22/2020, 12; *Johannes* ZD-Aktuell 2020, 07114; *Lachenmann/Berthold* ZD-Aktuell 2020, 07053; *Müller* ZD-Aktuell 2020, 7072; *Roßnagel* ZD-Aktuell 2020, 07118; zur App ferner *Kühling/Schildbach* NJW 2020, 1545).

Videotelephony, new for many, also continues to pose challenges to data protection specialists. Whether for work, school, or for leisure, video conferencing is being used nationwide for the first time to keep the lines of communication open in the pandemic.

The religious association *Jehovas Zeugen in Deutschland*, K. d. ö. R. also made its religious services available using the *Zoom* video platform to enable believers and interested persons to meet for worship. For data protection, this procedure had the advantage of not having to trace infection chains because of attending a religious service. Attendance lists were also not necessary. Using video conferencing for religious services enables data minimization, thus observing data protection principles.

The corona pandemic has clearly shown that there are many vital interests requiring protection, aside from data protection. Nevertheless, it has also shown that an approach suited to each particular situation, oriented on the principle of proportionality, is required from legislative, administrative and judicial authorities (*Gola/Klug*, Die Entwicklung des Datenschutzrechts [The Development of Data Protection Law], NJW 2020, 2774 Rn. 25).

⁴ *Strauß* K & R 2020, 325; *Roßnagel* ZD-Aktuell 2020, 07116; BfDI, www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/Gesundheit_Soziales-node.html; *Schomberg/Stroscher* ZD-Aktuell 2020, 07074

1.4 ePrivacy Regulation

This activity report also briefly presents the current stage of proceedings on 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 communication and repealing Directive 2002/58/EG).

As mentioned in the previous report, the ePrivacy Regulation is still the component missing in the EU data protection legal framework.

Concerning the ePrivacy Regulation, the Croatian Council Presidency suggested amendments to the draft regulation on February 21, 2020, and further amendments were suggested on March 6, 2020.

The government of the Federal Republic of Germany stated that it would not support these amendments during German Council Presidency, and was also unable to estimate when the ePrivacy Regulation could be expected to be passed at the earliest (answer of the national government to the parliamentary question regarding the European ePrivacy Regulation, Bundestag printed document no. 19/22244 of September 9, 2020).

Only a few days after the start of the German Presidency on July 6, 2020, the national government presented a first draft of a new ePrivacy Regulation for discussion, which was based on the compromise suggested by the Croatian Presidency of March 6, 2020, but containing quite striking amendments and variations (Stiegler MMR 2020, 641). The German draft attached particular importance to the fact that even in a European data protection regulation to electronic communication, entrepreneurial freedom must not be neglected.

On November 4, 2020, the German Presidency presented a new draft regulation, on which, however, no agreement could be reached.⁵

Our supervisory authority is greatly interested in the proceedings, even though it is currently impossible to say when a draft can be expected that will get a workable majority. The next activity report will continue to monitor the proceedings.

⁵ Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT&from=EN.

1.5 German Federal Data Protection Act (BDSG)

In April 2017, the national government passed the German Federal Data Protection Act (BDSG-new) as Article 1 of DSAnpUG-EU (Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680). The new Federal Data Protection Act came into force with the GDPR.

On November 26, 2019, the second Act to Adapt and Implement Data Protection Law EU came into force.

The amendments affecting religious data protection were discussed in the 2019 Activity Report. Our authority has not detected any changes to the position in 2019.

1.6 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. In view of the pandemic, it is noticeable that there were more inquiries concerning digital data protection. The Data Protection Authority also dealt with cases where data subjects received a letter from one of Jehovah's Witnesses who was taking part in the preaching activity. In all cases the data subjects' issues were dealt with and clarified.

2.2 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 the Activity Reports of 2018 and 2019 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.

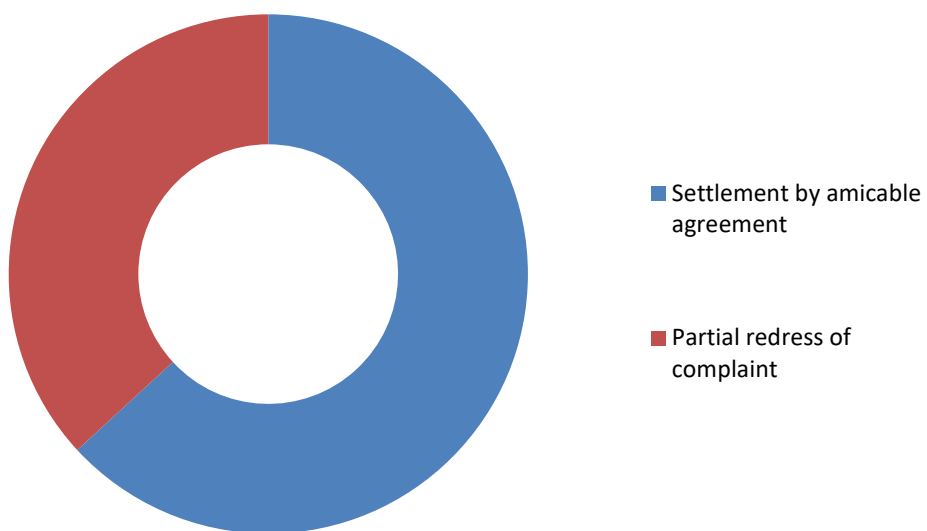
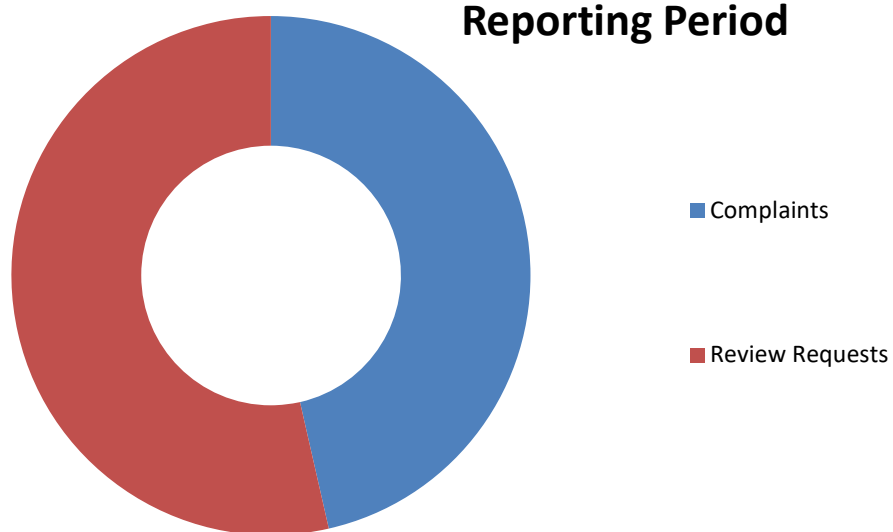
In ten cases, the complaint was dealt with by settlement. In three other cases, the activity of the Data Protection Authority led to partial remedy of the complaint.

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:

Complaints & Review Requests during the Reporting Period



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.

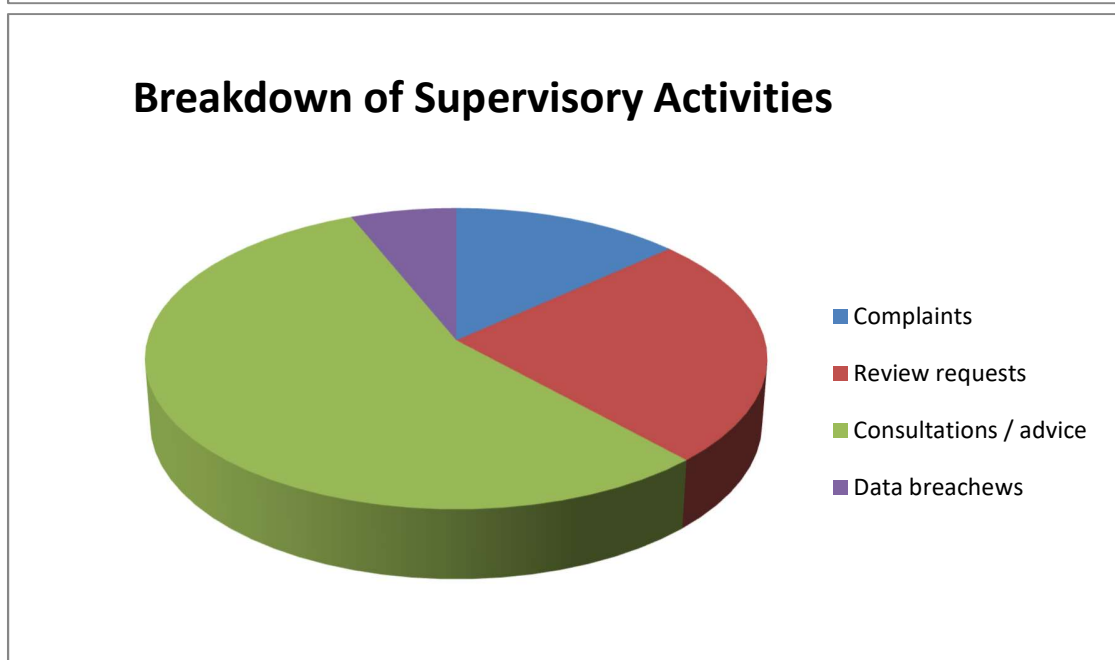
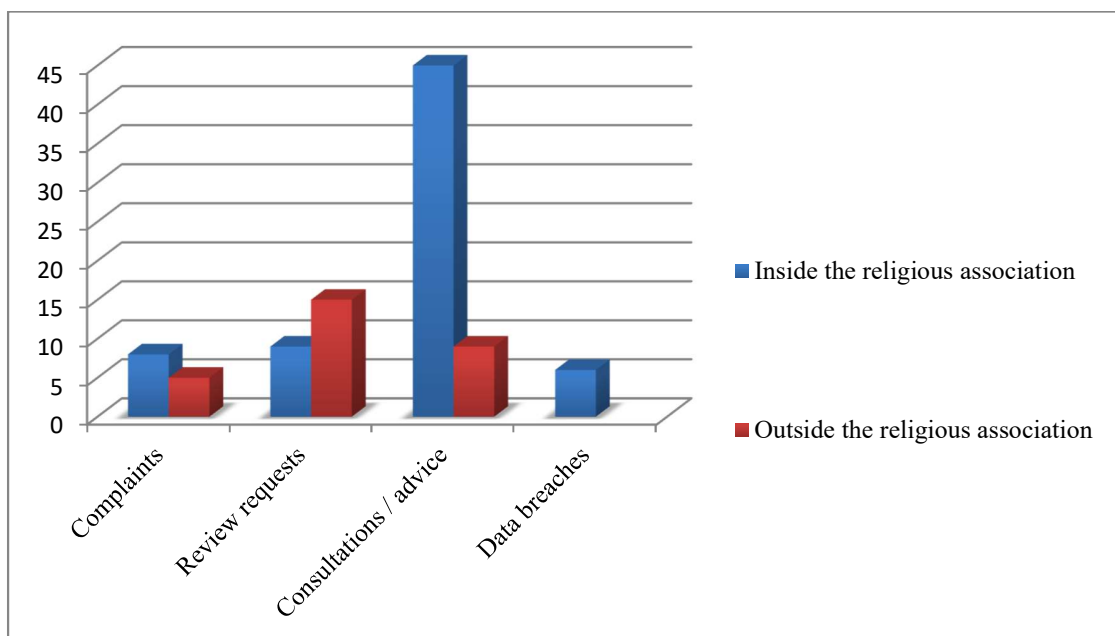
Adjustments in data security were also achieved in consultations. This included ecclesiastical proceedings.

Data Breaches:

In six 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:



3.1 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.

3.2 Website

The website of the *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 the current state of ecclesiastical as well as secular data protection law.

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 minimization**

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.
- **Personal data**

Personal data are individual details about personal or factual circumstances of a specific or identifiable natural person (data subject).
- **Privacy-by-design/default**

Privacy by design means data protection by technical design. The thought behind this is that data protection is best maintained in data processing operations when it is integrated in the development of these operations from the start.
Privacy by Default means data protection by privacy-friendly default settings.
- **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).