DATA PROTECTION AUTHORITY JEHOVAH'S WITNESSES

Activity Report 2022

Activity Report – 2022

of the *Data Protection Authority of Jehovah's Witnesses.*

The *Data Protection Authority of Jehovah's Witnesses* is required to submit an annual report on the results of its activities to the Branch Committee and the public (Section 24(6) of the Data Protection Act of Jehovah's Witnesses). This report covers the period from January 2022 to December 2022.

The annual report is available on our website; see:
https://datenschutz-jehovaszeugen.de/download/

LEGAL NOTICE

Publisher: *Jehovah's Witnesses Data Protection Authority*

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

Submitted in February 2026

Table of Contents

NOTE:

The glossary at the end of the annual report provides a list of definitions for various technical terms. When a term (e.g., personal data) appears for the first time in the text and is highlighted in color, this indicates that it is explained in more detail in the glossary.

List of Abbreviations

Par.	Paragraph
DSGJZ	Jehovah's Witnesses Data Protection Act
GDPR	European General Data Protection Regulation
EDSA	European Data Protection Board
EU	European Union
ECJ	European Court of Justice
Public-law corporation	Public-law entity
AI	Artificial Intelligence
SCC	Standard Contractual Clauses
TKG	Telecommunications Act
TMG	Telemedia Act
TTDSG	Telecommunications, Telemedia, and Data Protection Act
UK	United Kingdom
US	United States

Introduction

Throughout 2022, the effects of the SARS-CoV-2 virus have influenced the data protection work of the *Jehovah's Witnesses' data protection authority*.

The changes already introduced in 2020—such as the suspension of in-person divine services and the delivery of sermons to members of the faith primarily via mail —continued into 2022. The challenge remained to balance, on the one hand, the interests of the members and their associated freedom of religion, while on the other hand maintaining a consistently high level of data protection and—where necessary—further improving it. In March 2022, in-person worship services resumed, and public preaching resumed in June 2022, though written communication was maintained.

In general, new technological developments, particularly in the field of artificial intelligence (AI), have reignited the discussion about data protection and digital self-determination. The reporting period was marked by key developments and the challenge of evaluating new technologies, controlling international data flows, and protecting the rights of data subjects. This concerned, among other things, topics such as:

- Telecommunications and Telemedia Data Protection Act (TTDSG)
- AI Regulation (AI Act)
- Expiration of the SCC transition period
- US data transfers
- Data exports to the UK

The role of a data protection supervisory authority is to monitor compliance with data protection laws in order to protect individuals' fundamental rights. Due to digitalization and the increasing use of new technologies, ensuring this protection is particularly important for data subjects. The rights of data subjects granted by the DSGJZ continue to provide effective protection for their personal data during the 2022 reporting period. The fact that individual legal positions can be derived from the relevant legal bases, combined with the steadily growing societal interest in data protection and increasing awareness of the need to protect personal data, makes the DSGJZ a highly effective legal protection instrument.

Under the GDPR, all independent data protection supervisory authorities are required to apply the provisions of the Regulation uniformly. In Europe, this is ensured by the European Data Protection Board (EDPB) and its expert subgroups. It is therefore not surprising that interest in data protection issues remains high. During the reporting period, the *Jehovah's Witnesses Data Protection Oversight* also handled a wide range of advisory tasks, responding to inquiries from the religious community and its members as well as from third parties. A large number of inquiries regarding preaching by mail were received, which the *Jehovah's Witnesses Data Protection Oversight* was able to address.

In 2022, the *Jehovah's Witnesses' Data Protection Oversight* continued to pursue the goal of ensuring general awareness of personal data protection and adherence to data protection standards. Data protection begins with each data subject who knows and exercises their rights. An understanding and awareness that data processing involves data protection concerns is equally essential for the effective protection of informational self-determination.

One of the central tasks of *the Jehovah's Witnesses Data Protection Authority* is to strengthen data protection as an effective tool for the trustworthy and responsible handling of personal data. This creates the foundation for fair and transparent interaction among all parties involved while also enabling the preservation of pastoral confidentiality where necessary. This level of protection must also be ensured in digital contexts—a challenge that brings new risks and requires careful consideration. To meet these high standards, the DSGJZ has once again proven itself to be an effective and proven regulatory framework during the reporting period.

We present our activity report for the year 2022 below. Although the reporting period encompasses numerous developments and relevant decisions in general data protection, this activity report deliberately focuses on topics directly related to the religious community as well as on central aspects of religious data protection. For further information on general data protection, please refer to the activity reports of the state supervisory authorities.

We extend our gratitude to all those who are committed to implementing data protection, safeguarding the rights of data subjects, and taking into account the specific requirements of religious data protection.

Berlin, February 2026

Andreas Schlack
Board Member

1. Key Areas

1.1 National Law

The GDPR has been directly applicable in all EU member states since May 25, 2018. Member states harmonize the right to the protection of personal data under the GDPR with the right to freedom of expression and freedom of information through legislation (Art. 85 and Art. 86 GDPR). In general, Member States are not permitted to weaken or strengthen the data protection established by the GDPR through national regulations. However, the GDPR contains enabling clauses that allow individual Member States to regulate certain aspects of data protection on their own at the national level. There is therefore a need for regulation both with regard to the GDPR's enabling clauses and due to the need to harmonize national data protection law.

1.1.1 TTDSG

In May 2021, the German Bundestag passed the TTDSG ([1]). This law on data protection in electronic communications entered into force on December 1, 2021, simultaneously with a revised version of the TKG. These two reforms closed existing gaps in data protection and implemented the European Electronic Communications Code (Directive (EU) 2018/1972 (EECC Directive))[2] .

The coexistence of the GDPR, TMG, and TKG led to legal uncertainty among consumers who use telemedia and telecommunications services, among providers of these services, and among supervisory authorities. The TTDSG is intended to provide legal clarity and ensure effective data protection and privacy for end users. Numerous data protection provisions from the TKG and TMG have been consolidated into a single law for this purpose.

Unlike regulations (such as the GDPR), directives do not have direct regulatory effect. Directives must first be transposed into national law by the member states.

In Germany, however, the implementation of the ePrivacy Directive[3] had not been carried out as required. A formal act transposing the ePrivacy Directive, as amended by Directive 2009/136/EC[4] , was not included in the TMG. In particular, there had been no act transposing Article 5(3) of the ePrivacy Directive into German law at all. The previous dispute over whether an interpretation of the TMG compliant with the Directive was possible or not was declared closed by the Federal Court of Justice (BGH 28 May 2020 I ZR 7/16[5]) with the ruling that "the opt-out solution implies a requirement for consent."

Above all, the TTDSG's clarification regarding the requirement for consent to set cookies is essential. According to Section 25(1) of the TTDSG, cookies may generally only be set if the end user

[1] https://www.gesetze-im-internet.de/ttdsg/TTDSG.pdf
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018L1972
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX%3A32002L0058
[4] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009L0136
[5] https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Zivilsenate/I_ZS/2016/I_ZR___7-16A.pdf?__blob=publicationFile&v=1

has given their consent. This consent requirement does not apply in the cases specified in Section 25(2) of the TTDSG. Technically necessary cookies, for example, do not require consent.

A new provision concerns consent management services, also known as “Personal Information Management Services” (PIMS) or single sign-on solutions. Here, users can determine in a central location whether they wish to give consent to tracking.

1.2 European Union

As with the standardization of national data protection law, technical development also serves as the "pacesetter for data protection law" at the European Union level. Global networking and the internet are not bound by national borders and necessitate international regulation of data protection law (*Taeger/Gabel/Schmidt*, 4th ed. 2022, GDPR preamble Art. 1, para. 8).

1.2.1 AI Regulation

The release of ChatGPT in late 2022 marked a turning point: AI applications became suitable for mass use and moved to the center of the data protection debate.

During the 2022 reporting period, the regulation of artificial intelligence (AI) increasingly became the focus of European data protection policy. The planned EU AI Regulation (AI Act) was extensively discussed and further developed. The goal is a uniform legal framework that assesses the use of AI systems based on their risk potential while protecting fundamental rights, security, and transparency.

Particularly relevant for religious data protection is the classification of so-called high-risk AI systems, for example, in the processing of sensitive data. These systems will be subject to strict requirements in the future—including transparency obligations, human oversight mechanisms, and evidence of data quality.

The discussion surrounding the AI Regulation demonstrates that even in a religious context—such as in the management of personal data—new technologies must be carefully evaluated and deployed in compliance with data protection standards. The ethical standards that religious institutions apply to the handling of personal information align in many respects with the goals of AI regulation: protection of dignity, safeguarding of privacy, and responsible technology design.

1.2.2 SCC Transition

As explained in detail in the 2021 Activity Report, the transition to the SCC was imminent in 2022. By December 28, 2022, at the latest, all SCCs must have been transitioned to the version adopted by the European Commission in June 2021.[6] The 2021 SCCs feature a modular structure as well as new obligations for companies and can be concluded through an individual contract or as part of main contracts, such as in general terms and conditions.

[6] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de

In accordance with this new requirement, the previously existing contractual agreements have been amended accordingly.

1.2.3 U.S. Data Transfers

While data transfers to the U.S. currently rely mostly on the new SCCs, a long-awaited agreement on the new Privacy Shield was emerging. Even after the adequacy decision is adopted, criticism of a successor agreement persists, as the NGO "My Privacy is None of Your Business" (NOYB), led by data protection activist Schrems, has already announced legal action against the Privacy Shield 2.0, meaning it is likely that the matter will ultimately end up before the European Court of Justice (ECJ).

The draft decision is currently being reviewed by the European Data Protection Board (EDPB), and in the next step, the European member states must be consulted. The adequacy decision is not expected before spring 2023.

1.2.4 Data Transfers to the UK

On June 28, 2021, the European Commission issued two adequacy decisions. One decision concerns the adequacy of the level of data protection under the UK GDPR, and the other concerns the Law Enforcement Directive, i.e., the directive on data protection in law enforcement. The decisions were limited to a period of four years. Despite this limitation, the Commission may intervene at any time should the United Kingdom's data protection law no longer ensure an adequate level of data protection.

This means that data transfers between the EU and the United Kingdom will be possible until June 27, 2025. The only condition is that a level of protection comparable to that of the GDPR is guaranteed.

Following the UK's withdrawal, the UK Information Commissioner's Office has issued its own standard contractual clauses. Under the International Data Transfer Agreement (IDTA) and the International Data Transfer Addendum, data exchange between the UK and other third countries is possible. If personal data of EU citizens is transferred from the UK to other third countries, a comparable level of protection must also be ensured in those third countries.

The IDTA consists of standard contractual clauses comparable to those used in the EU.

- International Data Transfer Agreement (IDTA)

  A key feature of the IDTA is that it grants the parties greater flexibility when concluding the agreement. This is made possible by a broader scope of application, the option to enter into

a separate commercial agreement, and the incorporation of the terms of that agreement into the IDTA. Additionally, arbitration may be agreed upon in lieu of ordinary legal proceedings.

- International Data Transfer Addendum

  The International Data Transfer Addendum may be considered in addition to the EU Standard Clauses when a company wishes to transfer personal data from the United Kingdom to third countries.

  Under these provisions, a company is not required to use the IDTA in addition to the EU Standard Clauses.

  However, less effort would be involved if personal data were transferred directly from the EU to the third country.

It is also important to note when the contracts for data transfers with third countries were or will be concluded.

Existing contracts and those concluded by September 21, 2022, that still contain the old EU Standard Clauses may initially continue to be used. However, an adjustment must be made by March 31, 2024. The old EU Standard Clauses must be replaced either by the IDTA or by the new EU Standard Clauses in conjunction with the International Data Transfer Addendum.

If a contract is concluded between March 31, 2022, and September 21, 2022, either the old EU standard clauses, the IDTA, or the new EU standard clauses in conjunction with the International Data Transfer Addendum may be used.

Starting September 21, 2022, new contracts must use the IDTA or the new EU Standard Clauses in conjunction with the International Data Transfer Addendum.

1.3 Jehovah's Witnesses Data Protection Act (DSGJZ)

Shortly after being granted the status of a public-law corporation, the religious community enacted its own data protection law. This law first took effect on February 13, 2008, and in a revised form on April 1, 2011. The aim was to ensure that members of the religious community and all other affected parties could trust that their personal data would be handled securely.

On May 22, 2018, an amendment to the DSGJZ was published, which has been in effect since May 24, 2018.

The DSGJZ guarantees the same data subject rights as those provided for in the GDPR. Furthermore, Section 1(7) of the DSGJZ stipulates that the provisions of the GDPR must be applied mutatis mutandis as part of the DSGJZ where necessary.

2. Data Protection under Religious Law

2.1 *Data Protection Oversight of Jehovah's Witnesses*

The *Data Protection Oversight Body of Jehovah's Witnesses* is tasked with ensuring compliance with the provisions of the DSGJZ and all relevant data protection regulations and with supporting their implementation (Section 24(1) DSGJZ).

In addition, pursuant to § 24(3) DSGJZ, the *Data Protection Oversight Body of Jehovah's Witnesses* has, among other things, the following responsibilities within its area of jurisdiction:

- It informs the public about risks, legal requirements, protective mechanisms and individual rights in connection with data processing and raises awareness of their significance (Section 24(3)(1) DSGJZ).
- It advises the branches and institutions of the religious community on legislative and administrative measures for the protection of personal data and the associated fundamental rights in relation to data processing (Section 24(3)(2) DSGJZ).
- It raises awareness among data controllers and processors regarding their obligations under applicable data protection law (Section 24(3)(3) DSGJZ).
- It receives and reviews complaints from data subjects, bodies or organizations and informs complainants within a reasonable timeframe about the status of the proceedings and the outcome (Section 24(3)(5) DSGJZ). An online form on the website of the Jehovah's Witnesses Data Protection Authority facilitates the submission of complaints.

The *Jehovah's Witnesses Data Protection Authority* continued to fulfill these duties during the reporting period. Due to the shift in the preaching methods of the congregation from personal door-to-door visits to a method that relied more on written correspondence, numerous submissions were made to the *Jehovah's Witnesses Data Protection Authority*.

- Testimonial Letters

A large number of affected individuals contacted the *Jehovah's Witnesses Data Protection Authority* and asked why they had received a personal letter from a Jehovah's Witness. These inquiries were answered in the vast majority of cases.

According to the *Jehovah's Witnesses Data Protection Authority*, local Jehovah's Witnesses used public sources (e.g., telephone directories) to address their personal letters.

In this way, the religious freedom of the believers was upheld while also taking into account the health considerations of all involved. No records were kept of this.

- Video Communication

In other cases, the *Jehovah's Witnesses Data Protection Authority* received inquiries regarding video communication platforms (such as "Zoom") during the 2022 reporting period.

At the start of the pandemic, the religious community decided, for health and safety reasons, that meetings would no longer take place in person but would be conducted via video conference.

Participants were not required to create their own user accounts or otherwise provide their personal data unless they wished to do so. It was up to each participant to decide whether to join via audio only or to also transmit a video feed from their camera into the video conference room.

For all inquiries, the *Jehovah's Witnesses' data protection office* was able to answer the questions raised by the individuals concerned.

2.2 Current Developments

The *Jehovah's Witnesses Data Protection Authority* also addresses proceedings by other state supervisory authorities to the extent that these relate to its own supervisory responsibilities.

In 2022, the *Jehovah's Witnesses Data Protection Authority* issued a decision:

- Facts of the case

The complainant is a Jehovah's Witness. The complaint is directed against *Jehovah's Witnesses in Germany*, a public-benefit corporation, and others. The complainant initially contacted his local congregation (the respondent) directly regarding the use of a digital bulletin board and subsequently contacted the *data protection oversight body of Jehovah's Witnesses* directly. In doing so, he pointed out that the processing of special categories of personal data on the operator's platform had not been carried out in accordance with applicable data protection laws; for example, that documents containing personal information were being processed without appropriate data protection safeguards.

The respondent was requested by the *Jehovah's Witnesses Data Protection Authority* to submit a statement. This was subsequently made available to the complainant with sufficient time to respond. In this regard, the complainant again contacted the *Jehovah's Witnesses Data Protection Authority* and further argued for the judicial enforcement of his claims.

Since the complainant's request was granted, the complaint proceedings were discontinued.

- Legal Assessment by the Authority

The complaint proceedings were discontinued because the complaint had already been resolved prior to its filing and therefore there was no longer a need for legal protection.

1. Resolution of the Subject Matter of the Complaint

According to the parties' consistent statements, the data concerning the complainant had already been completely deleted from the processing program in question prior to the filing of the complaint.

2. Legal Basis

Since the DSGJZ does not contain provisions regarding the resolution of a matter prior to the filing of a complaint, the relevant legal principles of the GDPR as well as those of the VwVfG/VwGO are applied (Section 1(6) and (7) DSGJZ).

These provide that complaints are to be examined only to the extent necessary and that an amicable settlement is to be sought as a matter of priority (Art. 57(1)(f); Recital 131 GDPR). In the case of settled proceedings, the case must be dismissed—as is the case with the right to object.

3. Application in the Context of Religious Law

These legal principles fit into the religious community's order, which is based on trust and care.

No particular interest in a declaratory judgment or risk of recurrence has been raised, nor is any apparent; use of the program has already been discontinued.

2.3 Cooperation with State Supervisory Authorities

In the interest of coherent data protection, the *data protection oversight body of Jehovah's Witnesses* seeks close coordination with state supervisory authorities, as provided for in Art. 57(1)(g) GDPR. This serves to ensure a uniform level of protection and to avoid divergent regulations with potentially adverse consequences for data subjects.

3. Facts and Figures

3.1 Statistics

The analysis of cases from the reporting period is presented in a structured format to highlight internal developments and enable comparability with other data protection reports. The presentation follows established standards of reporting practice.

With regard to the terms “complaint,” “data breach,” “suggestions for inspection,” and “consultations,” please refer to the explanations in previous activity reports.

Complaints

The Data Protection Authority reviewed and fully processed all complaints, requests for inspection, and reports of potential data protection violations submitted during the reporting period.

In fifteen cases, the complaints were resolved through settlement. In two additional cases, the actions of the data protection supervisory authority led to a partial resolution of the complaint.

In summary, it can be said that all proceedings before the data protection supervisory authority were concluded through decisions or amicable settlements.

In the remaining cases involving requests for review, no legal violations were found, or they could not be attributed to any specific individual.

Data Breaches

In 2022, no data breaches were reported to the *Jehovah’s Witnesses Data Protection Authority*.

Consultations

Pursuant to Section 24(3) of the DSGJZ, advising data controllers and raising awareness of data protection issues are among the central tasks of the data protection supervisory authority. During the reporting period, written and remote verbal consultations took place with a view to preventing data protection violations.

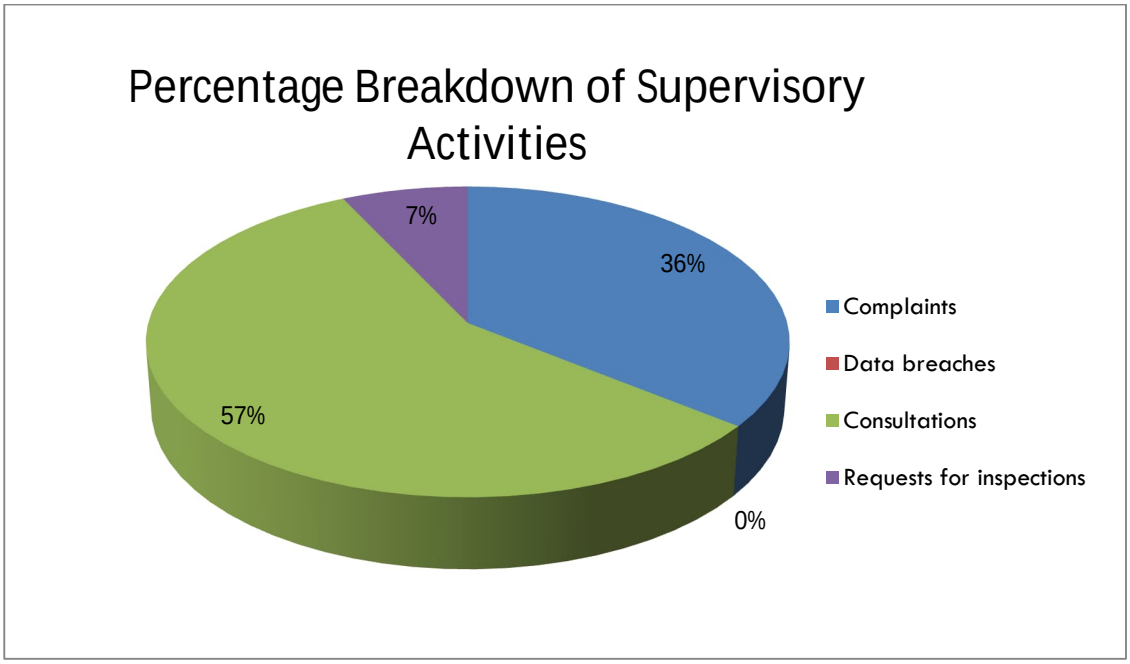
A particular focus was placed on the application of the DSGJZ, regarding which data controllers received regular support—for example, in designing processing operations in compliance with data protection regulations, in planning and conducting data protection impact assessments, and in providing advice on video surveillance.

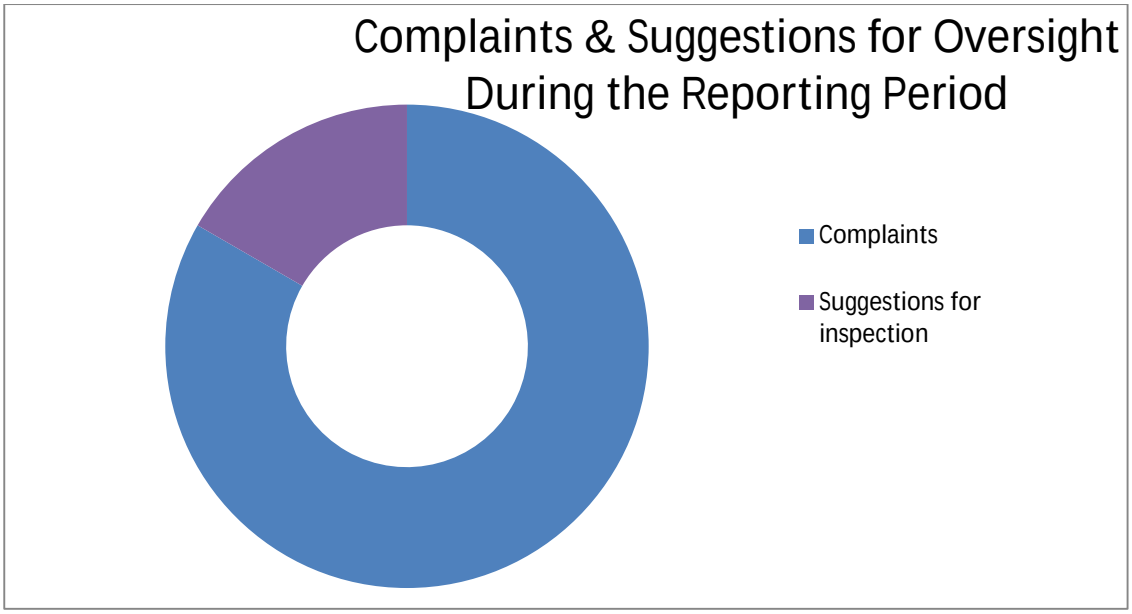
Through this preventive consultation, concrete improvements in data security were achieved in many cases. This also applied to procedures related to religious law.

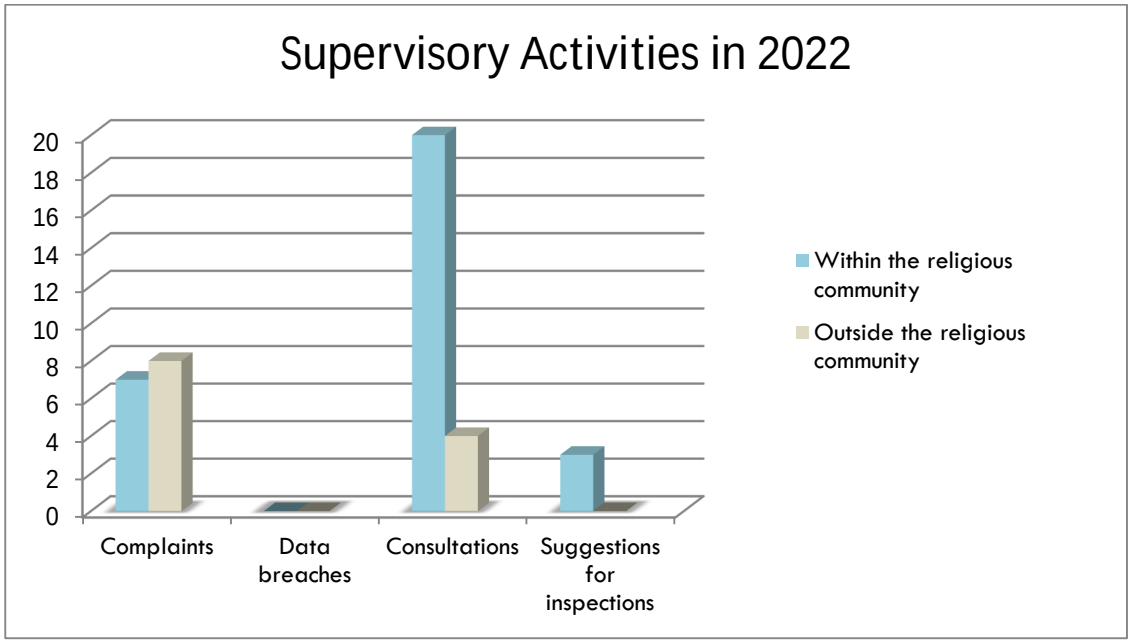
Initiations of Investigations

In 2022, the *data protection supervisory authority for Jehovah's Witnesses* initiated inspection recommendations in three cases.

Taking into account the aforementioned categories, the following graphical analyses emerge regarding the activities of the data protection supervisory authority during the reporting period:






Supervisory Activities in 2022
20
18
16
14
12
10
8
6
4
2
0
Complaints
Data breaches
Consultations
Suggestions for inspections
Within the religious community
Outside the religious community

3.2 Infrastructure

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

Grünauer Straße 104, 12557 Berlin

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

3.3 Website

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

https://datenschutz-jehovaszeugen.de

and is available 24 hours a day.

In addition to submitting a report in writing or by phone, every visitor to the website has the option of sending their inquiry to the *Jehovah's Witnesses Data Protection Authority* via an electronic reporting form.

4. Glossary

- DSGJZ — Jehovah's Witnesses Data Protection Act – The Jehovah's Witnesses Data Protection Act is also part of religious law. This act regulates the processing of personal data by the Jehovah's Witnesses religious community.
- GDPR — 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, on the free movement of such data, and on the repeal of Directive 95/46/EC) of 2016 standardizes the rules governing the processing of personal data by companies, public authorities, and associations within the European Union. The handling of data is clarified in eleven chapters comprising a total of 99 articles.
- Personal Data — Personal data consists of specific information regarding the personal or factual circumstances of an identified or identifiable natural person (data subject).
- Religious Law — The law established by the religious community itself for the organization and administration of its own affairs (e.g., the religious community's bylaws, the Jehovah's Witnesses' Data Protection Act).