Rules of Procedure for the *Datenschutzaufsicht Jehovas Zeugen* (VO-DSAJZ-E)

Version of December 6, 2023 in force since December 13, 2023 (Official Gazette of *Jehovas Zeugen in Deutschland*, No. 6, 2023, pp. 1 ff.)

§ 1 Scope of application. (1) The purpose of these Rules of Procedure is to regulate the activities under public law of the Data Protection Supervisory Authority of Jehovah's Witnesses in accordance with Article 91 paragraph 2 of the General Data Protection Regulation (GDPR) and § 23 Data Protection Act of Jehovah's Witnesses (DSGJZ).

(2) The provisions of these Rules of Procedure are based on the provisions of the religious association of *Jehovas Zeugen in Deutschland*, K. d. ö. R. (Statutes of the Religious Association *Jehovas Zeugen in Deutschland*, K. d. ö. R. (StRG), Preamble, (paragraph 4), and the principles of the rule of law in countries where the GDPR applies, as expressed in governmental laws on administrative procedure and the activities of governmental data protection supervisory authorities.

(3) If it becomes apparent in the course of proceedings that the Rules of Procedure must be supplemented in order to settle unresolved issues or guarantee a fair procedure, the Data Protection Supervisory Authority may analogously apply other provisions of ecclesiastical law and, if appropriate, the procedural rules of state administrative law.

§ 2 Data protection administrative procedures. For the purpose of these Rules of Procedure, data protection administrative procedures are activities of the Data Protection Supervisory Authority that have external effects and examine the requirements, the preparation and adoption of administrative acts that take the form of administrative rulings or other legally binding decisions. Such procedures presuppose a subjective legal right.

§ 3 Content of complaints. (1) If the Data Protection Supervisory Authority takes action as outlined in § 2, a complaint must contain:

1. details on the identity of the complainant and proof of identity (usually a certified signature or clearly legible copy of his identity card – the non-personal information can be redacted), unless the complainant already provided this proof in a previous procedure,
2. details on the identity of an authorised representative who shall provide written proof of his power of attorney upon request,
3. a description of the right considered to have been infringed,
4. a description of the entity or natural person that is deemed to be responsible for the alleged infringement (respondent to the complaint),
5. the facts upon which the infringement is based,

6. the grounds on which unlawfulness is alleged,

7. a request to establish that the alleged infringement has been committed, and

8. the details necessary to assess whether the complaint was filed in good time.

(2) Concerns anonymously raised with the Data Protection Supervisory Authority may result in the initiation of general data protection administrative procedures pursuant to § 4.

§ 4 General data protection administrative procedures. (1) Regardless of the opening of a data protection administrative procedure pursuant to § 2, the Data Protection Supervisory Authority can take measures outside of such administrative procedures in order to fulfil its obligations under §§ 24 and 25 DSGJZ if it becomes aware of a situation that requires action.

(2) Even if a procedure pursuant to paragraph 1 is initiated on the basis of anonymous reports or personal complaints, there is no subjective legal claim to participate in such a procedure or right to be informed of measures that have been taken and with what result, unless someone is personally affected.

(3) The Data Protection Supervisory Authority decides after due consideration whether and when to instigate a general data protection procedure. This does not apply when it by law, particularly the provisions of the DSGJZ,

1. must act ex officio or upon application,

2. can only act upon application and no such application was submitted.

§ 5 Language of the administrative procedure. (1) The administrative procedure shall not be tied to specific forms when no legal provisions exist which specifically govern procedural form. It shall be carried out in an uncomplicated, appropriate and timely fashion. The language of the administrative procedure is German.

(2) If applications are made to the Data Protection Supervisory Authority in a foreign language, or petitions, evidence, documents and the like are filed in a foreign language, the Data Protection Supervisory Authority shall immediately require that a translation be provided. Where necessary the Data Protection Supervisory Authority may require that the translation provided be made by a certified or publicly authorised and sworn translator or interpreter. If the required translation is not furnished without delay, the Data Protection Supervisory Authority may, at the expense of the participant, itself arrange for a translation.

§ 6 Authorised representatives and advisers. (1) A participant may cause himself to be represented by a person authorised for that purpose. The authorisation shall empower the person to whom it is given to take all actions related to the administrative proceedings except where its contents indicate otherwise. The authorised person shall provide written evidence of his authorisation upon request.

Any revocation of authorisation shall only become effective vis-à-vis the Data Protection Supervisory Authority when received by it.

(2) Authorisation shall not be terminated either by the death of the person granting such authorisation, or by any change in his capacity to act or in his legal representative; when however appearing in the administrative proceedings on behalf of the legal successor, the authorised person shall upon request furnish written evidence of his authorisation.

(3) Where a person is appointed to act as representative in proceedings, he shall be the person with whom the Data Protection Supervisory Authority deals. The Data Protection Supervisory Authority may approach the actual participant where he is obliged to cooperate. If the Data Protection Supervisory Authority does approach the participant, the authorised representative is to be informed.

(4) A participant may appear in negotiations and discussions with an adviser. Any points made by the adviser shall be deemed to have been put by the participant except where the latter immediately contradicts them.

(5) Authorised representatives and advisers may be excluded from the proceedings if it is recognisable or feared that they do not show due respect for the religious work of the religious association and do not respect the customary duty to maintain peace within the religious association. The decision is final.

(6) Authorised representatives and advisers may be refused permission to make submissions if they are unsuitable to do so; they may be refused permission to make a verbal submission only if they are not capable of proper representation.

(7) Refusal of permission under paragraphs 5 and 6 shall also be made known to the participant whose authorised representative or adviser is refused permission. Acts relating to the proceedings undertaken by the authorised representative or adviser after such refusal of permission shall be invalid.

§ 7 Inspection of files by the parties. (1) At its own discretion, the Data Protection Supervisory Authority rules on requests to access files. In doing so, it takes into account the extent to which access is necessary in order to assert or defend the legal interests of the parties involved. Access to files does not include drafts of decisions or the work in directly preparing them.(2) The Data Protection Supervisory Authority is not obliged to permit access to files if that would impair the Data Protection Supervisory Authority from fulfilling its tasks properly, if disclosure of the contents of files would be detrimental to the interests of the religious association or if the matter must remain confidential, by law or due to its nature, because of the legitimate interests of the parties involved or of third persons.

§ 8 Evidence. The Data Protection Supervisory Authority shall make use of the evidence which it deems necessary to determine the facts of the case in accordance with its due discretion. In particular, it may:

1.obtain information of any kind,

2. hear parties, hear witnesses and experts, or obtain written or electronic comments from parties, experts and witnesses,

3. consult documents and files,

4. inspection.

§ 9 Hearing. (1) Before an administrative act affecting the rights of a participant may be executed, the latter must be given the opportunity of commenting on the facts relevant to the decision.

(2) A hearing may be dispensed with if it is not required by the circumstances of the individual case, in particular where:

1. an immediate decision appears necessary due to imminent danger or in the interest of the Religious Association of Jehovah's Witnesses,

2. the hearing would jeopardise compliance with a time limit relevant to the decision,

3. it is not intended to deviate from the factual information provided by a party in an application or statement to his disadvantage,

4. the Data Protection Supervisory Authority wants to issue similar administrative acts in larger numbers.

(3) A hearing shall be omitted if it is contrary to a compelling ecclesiastical interest.

§ 10 Electronic communication. (1) Insofar as the law of the religious association permits, the transmission of electronic documents is permissible provided the recipient establishes access for this.

(2) Where legal provisions stipulate that a document be in written form, this may be replaced by electronic form unless determined otherwise by a legal provision. The law of the religious association can stipulate that in this case the electronic document must bear a qualified electronic signature. Signing with a pseudonym that makes it impossible to identify the person holding a signature key is not permissible. The requirement of a qualified electronic signature can be waived in legal transactions between structural divisions and agencies of the religious association (§ 5 StRG).

(3) If an electronic document sent to the Data Protection Supervisory Authority is not suitable for processing by that authority, it must inform the sender immediately, stating the technical specifications that apply. If a recipient claims that he is unable to process the electronic document sent by the Data Protection Supervisory Authority, it must send it to him again in a suitable electronic format or as a written document.

§ 11 Time limits and deadlines. (1) The right to have data protection administrative procedures conducted upon application expires if the applicant does not submit the

application within one year of becoming aware of the event, but no later than three years after the alleged event took place. Late applications will be rejected.

(2) Sections 187 to 193 German Civil Code apply to the calculation of time limits, unless paragraphs 3 to 5 specify otherwise.

(3) A time limit set by the Data Protection Supervisory Authority begins the day after the announcement of the time limit, except when the person concerned is informed otherwise.

(4) If the end of a time limit falls on a Sunday, a public holiday or a Saturday, the time limit ends at the close of the next working day. This does not apply when the person concerned has been informed that the time limit ends on a certain day and has been referred to this provision.

(5) Time limits fixed by the Data Protection Supervisory Authority may be extended. Where such time limits have already expired, they may be extended retrospectively, particularly when it would be unfair to allow the legal consequences resulting from expiration of the time limit to continue.

§ 12 Deciding on a complaint. (1) If the respondent remedies the alleged infringement of rights before the conclusion of the procedure with the Data Protection Supervisory Authority by complying with the complainant's requests and the Data Protection Supervisory Authority considers his complaints to be settled, the Data Protection Supervisory Authority must hear him on the matter. At the same time, the complainant must be notified in no particular form that the Data Protection Supervisory Authority will discontinue a procedure if he fails to demonstrate a legitimate interest in the continuation of the procedure within a reasonable period of time set by the Data Protection Supervisory Authority by providing reasons as to why he still considers the original infringement allegation to be, at least partially, unremedied. If such a statement from the complainant changes the substance of the matter, the original complaint will be withdrawn and a new complaint simultaneously filed. In this case, too, the original complaint procedure must be discontinued and the complainant must be informed in no particular form. Late statements are not considered.

(2) The Data Protection Supervisory Authority must inform the complainant of the status or outcome of the data protection administrative procedure within three months of receiving the complaint.

(3) The administrative act must be issued in writing and must be justified. In exceptional cases, in particular in cases of urgency, it may also be issued in text form or orally. An administrative act issued orally must be confirmed in writing and accompanied by a statement of reasons; an administrative act issued in text form must be accompanied by a statement of reasons.

(4) The statement of reasons shall state the essential factual and legal reasons that led the ecclesiastical Data Protection Supervisory Authority to its decision. The

justification of discretionary decisions should also reveal the aspects on which the Data Protection Supervisory Authority has proceeded in exercising its discretion.

(5) At least a summary statement of reasons shall be required:

1. insofar as the person for whom the administrative act is intended or who is affected by it is already aware of the opinion of the Data Protection Supervisory Authority on the factual and legal situation or is easily recognisable to him without justification,

2. if the Data Protection Supervisory Authority issues similar administrative acts in large numbers and the justification is not required according to the circumstances of the individual case,

3. if this results from an ecclesiastical or state legislation.

(6) A justification is not required if the Data Protection Supervisory Authority complies with an application or follows a declaration and the administrative act does not interfere with the rights of another.

(7) The Data Protection Supervisory Authority can correct clerical errors and similar obvious inaccuracies in an administrative act at any time. If there is a legitimate interest on the part of the party concerned, it must be rectified. The ecclesiastical Data Protection Supervisory Authority is entitled to request the submission of the document to be corrected.

§ 13 Additional stipulations to an administrative act. (1) An administrative act which a person is entitled to claim may be accompanied by an additional stipulation only when this is permitted by law or when it is designed to ensure that the legal requirements for the administrative act are fulfilled.

(2) Notwithstanding the provisions of paragraph 1, an administrative act may, after due consideration, be issued with:

1. a stipulation to the effect that a privilege or burden shall begin or end on a certain date or shall last for a certain period (time limit);

2. a stipulation to the effect that the commencement or ending of a privilege or burden shall depend upon a future occurrence which is uncertain (condition);

3. a reservation regarding annulment;

or be combined with

4. a stipulation requiring the beneficiary to perform, suffer or cease a certain action (obligation);

5. a reservation to the effect that an obligation may subsequently be introduced, amended or supplemented.

(3) An additional stipulation may not counteract the purpose of the administrative act.

§ 14 Validity of an administrative act. (1) An administrative act shall become effective vis-à-vis the person for whom it is intended or who is affected thereby at the moment he is notified thereof. The administrative act shall apply in accordance with its tenor as notified.

(2) An administrative act shall remain effective for as long as it is not withdrawn, annulled, otherwise cancelled or expires for reasons of time or for any other reason.

(3) An administrative act which is invalid shall be ineffective.

§ 15 Invalidity of an administrative act. (1) An administrative act shall be invalid where it is very gravely erroneous and this is apparent when all relevant circumstances are duly considered.

(2) Regardless of the conditions laid down in paragraph 1, an administrative act shall be invalid if:

1. it is issued in written or electronic form but fails to show the issuing data protection supervisory authority;
2. it has been issued by a data protection supervisory authority acting beyond its powers.

(3) An administrative act shall not be invalid merely because:

1. a data protection supervisory authority required by law to play a part in the issuing of the administrative act did not take or did not have a quorum to take the necessary decision;
2. the collaboration of another data protection supervisory authority required by law did not take place.

(4) If the invalidity applies only to part of the administrative act it shall be entirely invalid where the invalid portion is so substantial that the Data Protection Supervisory Authority would not have issued the administrative act without the invalid portion.

(5) The Data Protection Supervisory Authority may ascertain invalidity at any time ex officio; it must be ascertained upon application when the person making such an application has a justified interest in so doing.

§ 16 Making good defects in procedure or form. (1) An infringement of the regulations governing procedure or form which does not render the administrative act invalid under § 15 shall be ignored when:

1. the application necessary for the issuing of the administrative act is subsequently made;
2. the necessary statement of grounds is subsequently provided;

3. the necessary hearing of a participant is subsequently held;

4. the necessary collaboration of another data protection supervisory authority is subsequently obtained.

(2) Actions in line with paragraph 1 can be carried out until the final factual instance of religious judicial or administrative proceedings have been concluded.

(3) Where an administrative act lacks the necessary statement of grounds or has been issued without the necessary prior hearing of a participant, so that the administrative act was unable to be contested in good time, failure to observe the period for legal remedy shall be regarded as unintentional. The event resulting in restoration of the status quo ante under § 18 (2) shall be deemed to occur when omission of the procedural action is made good.

§ 17 Resumption of proceedings. (1) The Data Protection Supervisory Authority shall, upon application by the person affected, decide concerning the annulment or amendment of a non-appealable administrative act when:

1. the material or legal situation basic to the administrative act has subsequently changed to favour the person affected;

2. new evidence is produced which would have meant a more favourable decision for the person affected;

3. there are grounds for resumption of proceedings under section 580 of the Code of Civil Procedure.

(2) An application shall only be acceptable when the person affected was, without grave fault on his part, unable to enforce the grounds for resumption in earlier proceedings, particularly by means of a legal remedy.

(3) The application must be made within three months, this period to begin with the day on which the person affected learnt of the grounds for resumption of proceedings.

(4) The decision regarding the application shall be made by the Data Protection Supervisory Authority.

§ 18 Restoration of the status quo ante. (1) Where a person has through no fault of his own been prevented from observing a statutory time limit deadline regulated by these Rules of Procedure, he will, upon request, be granted a restoration of his original legal position. The fault of a representative is deemed to be that of the person he represents.

(2) The application must be made within two weeks of the removal of the obstacle. The grounds justifying the application must be substantiated when the application is filed or during the procedure connected with the application. The action that failed to be carry out must take place within the application period. If this is done, restoration may be granted even without application.

(3) After one year has elapsed from the end of the time limit which was not observed, no application for restoration may be made and the action not carried out cannot be made good.

(4) The application for restoration is decided upon by the Data Protection Supervisory Authority.

(5) Restoration is not permitted when this is excluded by legal provision.

§ 19 Serving administrative decisions. (1) Administrative decisions must be served in accordance with the provisions of the German Act on Service in Administrative Procedures (VwZG).

(2) During a procedure, the complainant must ensure that notifications from the Data Protection Supervisory Authority can contact him, in particular, he must report any change of address as soon as possible. The complainant can also name an authorised recipient and must accept service through this person.

(3) If the complainant does not comply with the obligation in paragraph 2 and if the new address cannot be ascertained, he must accept notifications and informal communications through the last address known to the Data Protection Supervisory Authority. If something cannot be delivered to the complainant for this reason, it is deemed to have been served upon posting, even if it is returned as undeliverable.

§ 20 Information on legal remedies. (1) An administrative act issued in writing or in text form which is subject to challenge shall be accompanied by a statement informing the party concerned of the possibility to appeal against the administrative act, of the Data Protection Supervisory Authority or of the court to which the appeal is to be lodged, the seat and of the time limit to be observed (information on legal remedies).

(2) Before appealing to the court, the complainant must give the Data Protection Supervisory Authority an opportunity to remedy his concerns if the complainant believes that the Data Protection Supervisory Authority failed to consider essential points when deciding on his application. The complainant must inform the Data Protection Supervisory Authority in writing within one month as to why he deems its decision to be incorrect. The Data Protection Supervisory Authority will then review its decision based on the notification and make a new decision within three months. If the complainant is not satisfied with the new decision, the complainant may then the appeal to the Berlin Administrative Court. In purely internal religious matters, state legal recourse is not available. If there is no notification from the complainant, the Data Protection Supervisory Authority considers the procedure closed.

(3) If legal recourse is available under state law, any data subject can apply to Berlin Administrative Court. This is also the case when the Data Protection Supervisory Authority remains inactive. Inaction is assumed when the Data Protection Supervisory Authority does not deal with the complaint or does not inform the data subject of the status or outcome within three months.

(4) The time limit for an appeal or other remedy shall begin to run only if the party concerned has been informed, in writing or electronically, of the appeal, the administrative authority or the court to which the appeal is to be lodged, the seat and the time limit to be observed.

(5) If the information is omitted or incorrectly given, the appeal may be lodged only within one year of notification or service, unless it was impossible to file before the expiry of the one-year period as a result of force majeure or if written or electronic information has been given to the effect that there is no appeal.

(6) The decision period in paragraph 2 does not include:

1. the time during which a procedure is suspended until the final decision on a preliminary question;

2. the duration of the procedure according to Articles 56, 60 and 63 GDPR.

§ 21 Data protection and secrecy. (1) The protection of personal data in data protection administrative procedures is governed by the current valid version of the DSGJZ as well as any legal provisions enacted by the religious association of Jehovas Zeugen in Deutschland, K. d. ö. R. to supplement and implement these Rules of Procedure.

(2) Participants are entitled to require that confidential information, particularly information pertaining to their personal life, as well as information of a pastoral nature, cannot be revealed by the Data Protection Supervisory Authority without permission.

(3) Pastoral secrecy must be strictly maintained (§ 1(8) DSGJZ).

§ 22 Clearly unfounded requests. (1) If the Data Protection Supervisory Authority concludes that a case fulfils the description in § 24(5) sentence 2 DSGJZ, it can demand payment of a reasonable fee from the applicant. When determining the fee, account is taken of the costs incurred by the application.

(2) The fee pursuant to paragraph 1 is a minimum of fifty euro and a maximum of two hundred and fifty euro.

§ 23 Entry into force. These Rules of Procedure enter into force upon publication in the Official Journal. They also apply to procedures already underway.