ZELICRA WARDEN

Data Processing Agreement

Version 1.1 · Last updated: 25 October 2026

This Data Processing Agreement ("DPA") forms part of the Warden Terms of Service between Zelicra Technologies Private Limited (CIN U62011KL2026PTC104927, registered office: Kalathiparambil, Chirakkakam, Varapuzha P.O., Paravur, Ernakulam, Kerala 683517, India) ("Zelicra", the processor) and the organisation that uses Warden ("you", the controller). It applies whenever Zelicra processes personal data on your behalf to provide Warden. You accept it when you accept the Terms; we will countersign a copy on request.

1. Definitions

"UK GDPR" and "Data Protection Act 2018" have their usual meanings, and together with any other UK law on personal data are the "Data Protection Laws". "Personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "special category data" have the meanings in the UK GDPR. "Customer Personal Data" means personal data that Zelicra processes on your behalf through Warden. "Sub-processor" means another processor that Zelicra engages to process Customer Personal Data.

2. Roles and scope

2.1 You are the controller and Zelicra is your processor for Customer Personal Data. The details of the processing are in Annex 1.

2.2 You are responsible for having a lawful basis for the Customer Personal Data you put into Warden, including a condition under Schedule 1 to the Data Protection Act 2018 for special category data and criminal offence data, for your instructions being lawful, and for giving data subjects the information the law requires.

2.3 Each party will comply with the Data Protection Laws that apply to it.

3. Instructions

3.1 Zelicra processes Customer Personal Data only on your documented instructions, including with regard to transfers outside the UK, unless UK law requires it to do otherwise; in that case Zelicra will tell you before processing, unless the law forbids that. The Terms, this DPA and your use and settings of Warden are your complete instructions; further instructions must be agreed in writing.

3.2 Zelicra will tell you immediately if, in its opinion, an instruction infringes the Data Protection Laws.

4. Confidentiality

Zelicra ensures that everyone it authorises to process Customer Personal Data is bound by a duty of confidentiality, and gives access only to the people who need it to provide and support Warden.

5. Security

Zelicra implements the technical and organisational measures in Annex 2, as required by Article 32 of the UK GDPR. It may change them as technology and threats change, but never so that the overall protection is reduced.

6. Sub-processors

6.1 You give Zelicra general authorisation to engage the sub-processors listed on our sub-processors page, as it stands at the date you accept this DPA (Annex 3).

6.2 Zelicra will email the managers of your home at least 30 days before adding or replacing a sub-processor. You may object on reasonable data protection grounds within that time. If we cannot resolve the objection, you may end the agreement, and Zelicra will refund any fees you paid for the period after it ends.

6.3 Zelicra imposes on each sub-processor, by written contract, data protection obligations that give the same protection as this DPA, and remains fully liable to you for each sub-processor's performance of them.

7. Data subjects' rights

7.1 Warden lets you view, correct, export and delete the records you keep, so you can respond to requests from data subjects. Zelicra will help you further, by appropriate technical and organisational measures, so far as that is possible.

7.2 If a data subject contacts Zelicra with a request or a complaint about Customer Personal Data, Zelicra will pass it to you without undue delay, and in any case within 5 working days so that you can acknowledge a complaint within the 30 days that section 164A of the Data Protection Act 2018 allows. Zelicra will not respond itself, except to tell the person that their request or complaint has been passed to you.

8. Assistance

Taking into account the nature of the processing and the information available to it, Zelicra will help you meet your obligations on security of processing, personal data breaches, data protection impact

assessments and prior consultation with the Information Commission, the UK's data protection regulator (UK GDPR Articles 32 to 36).

9. Personal data breaches

9.1 Zelicra will notify you without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting Customer Personal Data, by email to the managers of the affected home.

9.2 The notification will describe, so far as is then known, the nature of the breach, the categories and approximate number of data subjects and records concerned, its likely consequences, the measures taken or proposed to deal with it, and a contact for more information. Zelicra will send updates as it learns more, and will take reasonable steps to contain the breach and reduce its effects.

10. Deletion and return

10.1 While the agreement runs, a manager can download all Customer Personal Data for your home at any time, on the Your Data page.

10.2 When the account is closed or the agreement ends, you have 30 days to download your data or reopen the account. After those 30 days, Zelicra deletes all Customer Personal Data for your home, and it is removed from Zelicra's backups within the following 30 days, unless UK law requires Zelicra to keep it. Zelicra will confirm the deletion in writing on request.

11. Information and audits

11.1 Zelicra will make available to you all information needed to demonstrate compliance with Article 28 of the UK GDPR, and will allow for and contribute to audits, including inspections, by you or an auditor you appoint who is bound by confidentiality.

11.2 Audits take place on at least 30 days' written notice, during business hours, no more than once a year (unless a regulator requires one or a personal data breach has occurred), and at your cost. Zelicra may first answer with documentation, such as this DPA, our Security page and written answers to your questions, if that gives you what you need.

12. International transfers

12.1 Warden stores Customer Personal Data on our server in Helsinki, Finland, in the European Economic Area.

12.2 Zelicra is established in India, and its team accesses Customer Personal Data from India to provide and support Warden. You authorise these transfers. They are made under the safeguards set out in Annex 4.

12.3 Zelicra will not transfer Customer Personal Data to any other country outside the UK and the EEA, except to a sub-processor listed under clause 6 with the safeguards the Data Protection Laws require, or on your documented instructions.

13. Liability

Each party's liability to the other under this DPA is subject to the limits in the Terms of Service. Nothing in the Terms or this DPA limits either party's liability to data subjects or to the Information Commission.

14. Duration, precedence and changes

14.1 This DPA lasts for as long as Zelicra processes Customer Personal Data, and survives the end of the agreement until all Customer Personal Data has been deleted.

14.2 If this DPA and the Terms disagree about personal data, this DPA prevails. If the IDTA in Annex 4 conflicts with the rest of this DPA or with the Terms, Section 6.7 of the IDTA decides which terms apply.

14.3 Zelicra may update this DPA to reflect changes in the law or in Warden, giving at least 30 days' notice by email of any material change. No change may reduce the protection of Customer Personal Data without your agreement.

Annex 1: Details of the processing

Subject matter	Providing Warden, an online staff compliance records service for care homes.
Duration	The term of the agreement, plus up to 60 days for deletion (30 days to download or reopen, then up to 30 days for backups).
Nature of the processing	Hosting and storing records and documents; organising, displaying and retrieving them; sending emails and push notifications; producing reports, evidence packs and exports; backing up; deleting.
Purpose	To let you keep and evidence staff compliance records: policies and notices read and signed, training, recruitment checks, the DoLS register, supervisions and appraisals, reports for inspection, and notifications to staff.
Categories of data subjects	Your staff, including managers, employees, bank and agency workers, contractors and volunteers who use Warden or are recorded in it; job applicants and new starters whose recruitment checks are recorded; residents recorded in your DoLS register; other people named in your records, such as assessors, referees and residents' representatives.

Categories of personal data	Names, contact details (email address and phone number, which may be personal) and roles; sign-in history, IP addresses and push notification subscriptions; training records and certificates; job role, employment type and start date; recruitment checks, including proof of identity, DBS check details and certificate copies, references and evidence of conduct in previous employment, reasons earlier work with children or vulnerable adults ended, evidence of qualifications, employment history, whether the pre-employment health check is complete (not the health information itself), right to work checks and documents, and professional registration numbers; supervision and appraisal notes; notices, acknowledgements, signatures and comprehension answers; DoLS register entries (resident name, references, dates, local authority, assessor, the relevant person's representative, the outcome and any conditions, CQC notification details, review notes and documents); email delivery records; audit log entries.
Special category data	Health and mental capacity information in DoLS records, and any health information you choose to record in supervision notes or other notes. Protected by the measures in Annex 2.
Criminal offence data	DBS check details and certificate copies. Certificate copies are deleted 6 months after the certificate's issue date (or 6 months after the check was recorded, if no issue date was entered); the check record (reference, dates and result) is kept.
Frequency	Continuous, while you use Warden.
Retention	As set out in the retention table in our Privacy Policy.

Annex 2: Technical and organisational measures

- **Location:** one server in Hetzner's data centre in Helsinki, Finland; the database and uploaded documents stay on it.
- **Separation:** every record belongs to one care home and is looked up within the signed-in person's home; uploaded documents are stored outside the public web folder and served only after that check.
- **Access control:** managers sign in with a password stored as a bcrypt hash, with optional two-step verification (authenticator app and recovery codes); staff sign in with single-use links stored as hashes; separate manager and staff permissions.
- **Sessions:** end after 60 minutes of inactivity and after 12 hours in any case; a password change ends the person's other sessions; sign-in, reset and two-step attempts are rate-limited.
- **Encryption in transit:** HTTPS only, TLS 1.2 and 1.3, HSTS for one year; emails sent to Brevo over an encrypted connection; push notifications encrypted end to end.
- **Application security:** security tokens on every form; an enforced Content Security Policy; framing by other sites refused; spreadsheet exports protected against formula injection.

- **Logging:** an audit log of sign-ins (including failures), security changes, exports, downloads and changes to records, with time and IP address, which managers can view.
- **Server:** firewall allowing only web traffic and administrative access; administrative access by SSH key only, with repeated failures blocked; daily automatic operating system security updates; scheduled jobs run with the application's restricted account.
- **Backups:** nightly backups of the database and uploaded documents, each database backup restore-tested automatically; the last 30 kept. Currently on the same server; an encrypted copy in a second location is planned.
- **Deletion:** data export at any time; deletion 30 days after closure, and removal from backups within a further 30 days.
- **People and change control:** production access limited to the Zelicra engineers who run Warden, each with their own key, and sign-ins to the server logged; every change tested on a separate copy before release, with a recorded way to undo it.
- **Planned:** the dated roadmap on our Security page.

Annex 3: Sub-processors

The sub-processors authorised under clause 6.1 are those listed on our sub-processors page on the date you accept this DPA. On 10 October 2026 they are Hetzner Online GmbH (hosting, Helsinki, Finland) and Brevo CRM Solutions Private Limited (email delivery, servers in France and Belgium). Browser push services carry encrypted notifications to staff devices that have switched them on; they cannot read them and are not sub-processors. Warden's pages load fonts from Google Fonts, so Google receives the IP address and browser details of the person viewing a page, but no records; Google is not a sub-processor.

Annex 4: International transfers

4.1 Customer Personal Data is stored in Finland. When Zelicra's team in India accesses it to provide and support Warden, you (the exporter) transfer Customer Personal Data to Zelicra (the importer) under Chapter V of the UK GDPR. For those transfers, you and Zelicra enter into the International Data Transfer Agreement, version A1.0, issued under section 119A of the Data Protection Act 2018 by the Information Commissioner, now the Information Commission (the "IDTA"). It is incorporated into this DPA with the information in the table below. You and Zelicra agree to be bound by it when you accept the Terms, which is its start date.

Parties (Table 1)	Exporter: you, the organisation that holds the Warden account, identified by the name recorded in that account and, once you choose a plan, by the legal name, address and any registration number you give us for invoicing; your key contact is the manager who holds the account. Importer: Zelicra Technologies Private Limited (CIN U62011KL2026PTC104927), at its registered office above; key contact, and contact for data subjects: privacy@zelicra.com.
Law and claims (Table 2)	The IDTA is governed by the law of England and Wales, and legal claims are to be made in England and Wales.
Status (Table 2)	The exporter is a controller. The importer is the exporter's processor. UK GDPR applies to the importer's processing of the transferred data.
Linked Agreement (Table 2)	The Warden Terms of Service and this DPA, between you and Zelicra, from the date you accept them.
Term and ending (Table 2)	The importer may process the transferred data for the period for which the Linked Agreement is in force and, after it ends, until the transferred data has been deleted under clause 10 of this DPA. The parties cannot end the IDTA before the end of the term unless there is a breach of the IDTA or the parties agree in writing. If the Approved IDTA changes, the importer may end the IDTA as set out in its Section 29.2.
Onward transfers (Table 2)	The importer may transfer on the transferred data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 of the IDTA, but only to the authorised receivers set out in this DPA: the sub-processors authorised under clause 6 and listed in Annex 3.
Review (Table 2)	First review date: 10 October 2027. The parties will review the security requirements at least each year, and each time there is a change to the transferred data, the purposes, the importer's information or the transfer risk assessment.
Transferred data (Table 3)	The personal data, data subjects and purposes described in Annex 1, and any other purposes compatible with them. The transferred data includes data relating to physical or mental health and to criminal convictions and offences, as described in Annex 1. These categories update automatically if Annex 1 is updated.
Security requirements (Table 4)	The measures in Annex 2, which update automatically if Annex 2 is updated.

Extra protection clauses (Part 2)	(i) The transferred data stays stored in Finland and is reached from India only over encrypted connections. (ii) Only the Zelicra engineers who run Warden can reach it, each with their own credentials. (iii) None.
Commercial clauses (Part 3)	The Terms of Service and this DPA.
Mandatory clauses (Part 4)	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.

4.2 Zelicra has prepared a transfer risk assessment for these transfers (dated 10 October 2026), which you may rely on or use in your own. It concludes that, with the IDTA and the measures in Annex 2, the transferred data keeps a level of protection that is not materially lower than under UK law. Zelicra will send you a copy on request, review it at least once a year and whenever the law or practice in India changes in a way that could affect it, and tell you if its conclusion changes.

4.3 If a public authority asks Zelicra for access to transferred data, Zelicra will follow Section 23 of the IDTA: it will challenge the request where there are significant grounds to believe it is unlawful, tell you about it without undue delay where the law allows, and keep a written record of it.

This DPA was written by Zelicra to meet Article 28 of the UK GDPR. If your organisation needs changes, or a countersigned copy, email privacy@zelicra.com.