Data Processing Agreement

Between a business using Opdeck and Opdeck, under the Protection of Personal Information Act 4 of 2013 (POPIA)

THE RESPONSIBLE PARTY ("THE CUSTOMER")	THE OPERATOR ("OPDECK")
Business name: _____ Registration number: _____ Opdeck account name: _____ Contact person and email: _____	Opdeck, the field service platform at www.opdeck.co.za Information Officer: Keanu Email: keanujvv@gmail.com

1. Purpose and roles

1.1 The Customer uses Opdeck to run its field service work: customers, sites, job cards, quotes, invoices, assets and the documents that go with them. In doing so, the Customer places personal information on Opdeck.

1.2 For that personal information, the Customer is the **Responsible Party** and Opdeck is an **Operator**, as those terms are defined in section 1 of POPIA. The Customer decides why and how the information is processed; Opdeck processes it on the Customer's behalf to provide the service.

1.3 This agreement sets out the written terms required by sections 20 and 21 of POPIA. It forms part of, and is read with, the Opdeck Terms of Service. Where the two conflict on the handling of personal information, this agreement prevails.

2. What is processed

The personal information Opdeck processes for the Customer depends on what the Customer and its team enter, and typically includes:

Whose information	What information
The Customer's own customers and their site contacts	Names, phone numbers, email addresses, billing and site addresses, custom customer fields, and the GPS location of sites and assets where captured.
The Customer's team (owners, admins, technicians)	Names, email addresses, login details (passwords stored only as a secure hash), job assignments, time on site and travel records.
Anyone signing or appearing on a job card	Signatures, photographs taken on site, and names recorded on job cards, certificates of compliance and other attached documents.

2.1 Opdeck processes this information only to provide, secure, support and maintain the service for the Customer, including generating and sending job cards, quotes and invoices when the Customer's team asks it to.

2.2 Opdeck does not sell the Customer's information, does not use it to market to the Customer's customers, and does not use it for any purpose of its own.

3. Opdeck's obligations

3.1 Instructions. Opdeck processes the Customer's personal information only with the Customer's knowledge and authorisation (section 20(a)), which the Customer gives through its use of the service and its written requests.

3.2 Confidentiality. Opdeck treats the Customer's personal information as confidential and does not disclose it except as this agreement allows, or where the law requires it (section 20(b)).

3.3 Security. Opdeck maintains the technical and organisational safeguards described in Annex A, as required by sections 19 and 21, and reviews them as the service changes.

3.4 Security compromises. If Opdeck has reasonable grounds to believe the Customer's personal information has been accessed or acquired by an unauthorised person, it will notify the Customer immediately, and in any event within 72 hours of becoming aware of it (section 21(2)). The notice will say what is known about the compromise, the information affected and the steps taken, so the Customer can meet its own duties under section 22.

3.5 Requests from individuals. If a person asks Opdeck directly for access to, correction of or deletion of information the Customer holds about them, Opdeck will pass the request to the Customer promptly and help the Customer respond to it.

3.6 Demonstrating compliance. Opdeck will answer the Customer's reasonable written questions about how its information is handled, and provide the information reasonably needed to show compliance with this agreement.

4. Who at Opdeck can see the Customer's information

4.1 Access to customer data at platform level is limited to one named person: Opdeck's founder and Information Officer. No one else at Opdeck has that access.

4.2 That access is used only to give support the Customer has asked for (for example, building a job card template or investigating a fault), to keep the service running and secure, or where the law requires it.

4.3 Within the Customer's own account, what each team member can see and do is set by the role the Customer gives them (owner, admin or technician).

5. Service providers (sub-operators)

Opdeck uses the following providers to run the service. Each handles only what it needs to perform its part:

Provider	What it does	Where
Supabase	Hosts the main database: customers, sites, job cards, quotes, invoices and account records. Takes the daily backups.	Amazon Web Services, Ireland (EU), region eu-west-1
Vercel	Hosts the Opdeck application, and stores uploaded photos, signatures and documents (Vercel Blob).	Vercel's global infrastructure
Resend	Delivers emails the service sends: job cards, quotes and invoices emailed to the Customer's customers, and account emails.	United States
PayFast	Processes the Customer's Opdeck subscription payments. It receives billing details only, never job or customer data.	South Africa

Provider	What it does	Where
Browser push services	Deliver job notifications to team members' phones and browsers, through the provider built into each device (Google, Apple or Mozilla).	Provider of each device

5.1 Opdeck requires each provider to protect the information to a standard no lower than this agreement.

5.2 Before adding or replacing a provider that handles the Customer's personal information, Opdeck will give the Customer at least 30 days' notice by email. If the Customer objects on reasonable grounds and the matter cannot be resolved, the Customer may end its subscription without penalty.

6. Transfers outside South Africa

6.1 The Customer's database is stored in Ireland, in the European Union, where the General Data Protection Regulation applies. Some providers listed above are based in the United States.

6.2 Opdeck transfers personal information across borders only to providers that are subject to a law, binding corporate rules or a binding agreement giving an adequate level of protection, as section 72 of POPIA requires. The Customer agrees to these transfers for the purpose of providing the service.

7. Backups, retention and deletion

7.1 The database is backed up automatically every day by Supabase. Backups are encrypted and kept for a limited rolling period, after which they are overwritten.

7.2 While the Customer's account is active, its information is kept so the service can work. The Customer can download a full export of its job cards and records from Opdeck at any time.

7.3 When the Customer closes its account, or asks in writing for its information to be deleted, Opdeck will delete it from the live service within 30 days. Copies in backups are removed as those backups expire on the rolling schedule in 7.1, and are not restored except to recover the service.

7.4 Opdeck may keep information for longer only where the law requires it, and then only for as long as required.

8. The Customer's responsibilities

8.1 The Customer is responsible for having a lawful basis to collect the personal information it places on Opdeck, and for telling the people concerned how their information is used, as POPIA requires of a Responsible Party.

8.2 Opdeck works offline, so job information can be stored on the phones and tablets the Customer's team use until it syncs. The Customer is responsible for securing those devices, and for removing a team member's access when they leave.

9. Term and general

9.1 This agreement applies for as long as Opdeck processes personal information for the Customer, and its confidentiality and deletion terms continue after that until the information is deleted.

9.2 This agreement is governed by the laws of the Republic of South Africa.

9.3 Questions about this agreement, or about the Customer's information, go to Opdeck's Information Officer at keanujvv@gmail.com.

Signed

For the Customer	For Opdeck
Signature: _____	Signature: _____
Name: _____	Name: _____
Capacity: _____	Capacity: _____
Date: _____	Date: _____

Annex A: Security safeguards

The measures Opdeck has in place to protect the Customer's personal information (sections 19 and 21 of POPIA):

Area	What Opdeck does
Encryption in transit	All connections to Opdeck, and between Opdeck and its providers, are encrypted (HTTPS/TLS).
Encryption at rest	The database and its backups are stored encrypted by the hosting provider.
Passwords	Stored only as a secure one-way hash. Opdeck cannot see or recover a user's password.
Separation between accounts	Every request is limited to the signed-in user's own company account, so one business can never see another's records.
Roles within an account	Owners, admins and technicians each see and do only what their role allows. Billing, team and settings changes are limited to owners and admins.
Shared links	Job cards shared by link use long, unguessable addresses, created only when a team member chooses to share.
Platform access	Limited to one named person, used only for support the Customer requested, keeping the service running, or legal requirements (clause 4).
Backups	Automatic daily database backups, kept for a limited rolling period (clause 7).
Payments	Card details are entered with PayFast and never reach Opdeck's servers.
Incidents	Suspected compromises are investigated straight away and reported to the Customer within 72 hours (clause 3.4).

Opdeck reviews these measures as the service changes, and will tell the Customer of any change that lowers the level of protection.