Appwinst

Normative specification: Customer portal

Version 1.8 of 26 October 2026

1. Status, scope and conventions

This specification describes the apps of a company that installs and maintains heat pumps and ventilation at businesses and schools in Twente. This document calls that company the installation company (Terms). It was drawn up at the Fit check and is a draft until the Build brief records its version and digest (BB-001). It describes the Build the Fit check proposes; what it does not name is not part of the Build.

Scope. Two apps that work in the browser on desktop, tablet and phone (BC-011):

- the **Customer portal**, for the contacts of the installation company's relations, at `https://portal.voorbeeld.example`;
- **Office**, for the installation company's employees, at `https://office.voorbeeld.example`.

A customer signs in with a sign-in link, sees the orders of their relation with their status and planned date, opens an order with its work orders, invoice and documents, and asks a question about it. An office employee signs in with a passkey, answers that question with the order beside it, and the customer receives an e-mail. The questions and answers are the Messages add-on (A5). The app reads orders, order files, relations and contacts from Exact Online and writes nothing to it. Texts and images, Management area and Organisation management are in the Build (ADD-006). What the Build does not do is in the Not-list.

Conventions.

- **ALG-001** The words MUST, MUST NOT, SHOULD, SHOULD NOT and MAY have the meaning BCP 14 (RFC 2119 and RFC 8174) gives them when they appear in capitals.
- **ALG-002** Every requirement has a fixed code with a prefix per section. A code is never reused or renumbered; a withdrawn requirement keeps its code with the text "Withdrawn in version X.Y". A change after signing is a new version of this document, named in an Amendment (BB-010).
- **ALG-003** A code that this document does not itself define, such as LEG-019, is a requirement of the normative specification of Appwinst, in the version the Build brief records (VER-001). Where this document and the Build brief differ, the Build brief applies to price, dates and obligations, and this document to what the app does.

- **ALG-004** Every term from Terms means the same throughout this document, and one idea has one word.
- **ALG-005** Every setting of the app is in Appendix: configuration values, with the requirement that defines it. A different setting is a new version of this document (ALG-002). What the administrator manages in the Management area or in Texts and images, such as the document types per kind (GEG-006), is data of the app and not a setting: the administrator changes it without a new version.

Research basis

The journeys and requirements in this document rest on these sources, all read on 2026-10-26. Each source is listed here with publisher, title, site and date; the full address is in the research the Fit check keeps. The number in brackets, such as [20], is that of that research. This document cites a source by that number, or by its publisher and title as listed here. A source that no journey or requirement uses is not listed here, so the numbers are not consecutive. The sources [41] and [42] are named by the requirements themselves.

- [1] Exact Online, REST API: SalesOrderSalesOrders, start.exactonline.nl, undated.
- [2] Exact Online, REST API: overview of the resources, start.exactonline.nl, undated.
- [3] Exact Online, REST API: WebhooksWebhookSubscriptions, start.exactonline.nl, undated.
- [4] Exact Online, REST API: DocumentsDocuments, start.exactonline.nl, undated.
- [5] Exact Online, REST API: CRMContacts, start.exactonline.nl, undated.
- [6] Apideck, Exact Online configuration, apideck.com, undated.
- [7] Exact Knowledge Base, App publication procedure, exactonline.com, undated (read through a search result).
- [8] Exact Knowledge Base, Step 3. Get/use access tokens, exactonline.com, undated (only the search snippet read; the page did not load).
- [9] Nango, Exact Online, nango.dev, undated.
- [10] Hookdeck, Guide to Exact Online Webhooks, hookdeck.com, undated.
- [11] Clickker, Exact Online restrictions on entries and API calls, clickker.nl, undated (effective date 1 January 2025).
- [12] Barcode Scan, Exact Online API limits guide, barcodescan.nl, undated.
- [17] IPLO, Consumer file (completion file) and Wkb, iplo.nl, undated.
- [18] VBK, The Wkb completion file has entered into force retroactively, vbk.nl, 2024-03-07.

- [19] Kiwa, Wkb: consumer file only required for new works, kiwa.com, undated.
- [20] Baymard, Accounts & Self-Service UX Research 2026, baymard.com, 2026-09-09.
- [21] Baymard, Order Tracking UX: 6 Key Details to Provide, baymard.com, undated.
- [22] Baymard, Order Tracking & Returns UX Benchmark 2024, baymard.com, March 2024.
- [23] NN/g, Passwordless Accounts and A Checklist for Registration and Login Forms on Mobile, nngroup.com, undated.
- [24] NN/g, Visibility of System Status and Progress Indicators, nngroup.com, undated.
- [25] Buildertrend, Qobrix and Contractors Cloud, pages on customer portals for contractors, undated.
- [26] OutSmart knowledge base, Customer portal: work order settings, out-smart.com, undated.
- [27] Regulation (EU) 2016/679 (GDPR), Articles 5, 25, 28 and 32, 2016-04-27, in force.
- [28] Vlaamse Toezichtcommissie, Data processing agreement, vlaanderen.be, undated; and Apideck, Exact Online overview, apideck.com, undated.
- [29] Taylor Wessing, European Accessibility Act: requirements for e-commerce services, taylorwessing.com, 2025-09-30.
- [34] Chift, How to integrate with Exact Online API, chift.eu, undated.
- [35] Microsoft Power Users, "Old refresh token used", microsoft.com, undated.
- [36] Exact Support, API rate limits, exactonline.com, undated (read through a search result).
- [38] Peliqan, Exact Online API, peliqan.io, undated.
- [39] Genkgo, Setup of the connection (Exact Online), genkgo.com, undated.
- [40] Cyclr, Exact Setup, cyclr.com, undated.
- [41] W3C, Web Content Accessibility Guidelines (WCAG) 2.2, W3C Recommendation, w3.org, 2023-10-05.
- [42] OWASP, Application Security Verification Standard 5.0.0, owasp.org, May 2025.

Versions

Version	Date	What changed
1.0–1.3	up to and including 2026-10-19	Drawn up at an earlier Fit check, for a different Build request. Replaced by 1.4.

1.4	2026-10-26	Drawn up anew for the Build request of Fit check round 1, for the Build the Fit check proposes: the Customer portal and Office with questions about an order (A5), seven screens, three roles, one read-only integration with Exact Online. Contacts come through the integration, not from an import file (BUITEN-002). Planning maintenance is not part of the Build (BUITEN-003). No phone numbers (BUITEN-008). A code from 1.0–1.3 has in 1.4 only the meaning 1.4 gives it.
1.5	2026-10-26	The items of the Not-list are named BUITEN-001 to BUITEN-013 inclusive; in 1.4 they were named UIT-, with the same numbers and words, and every reference follows. Where a source outside the Research basis was cited with its date, its number from the research now stands, such as [27]. What the app does does not change.
1.6	2026-10-26	The requirements of the Domain model are named GEG-001 to GEG-015 inclusive; in 1.5 they were named DOM-, with the same numbers and words. They got a

		different prefix because the specification of Appwinst itself uses DOM-. Every reference follows. What the app does does not change.
1.7	2026-10-26	The names of the events for opened order files in REIS-003 are written without a second underscore. What the app counts and does does not change.
1.8	2026-11-02	The platform is now named Appwinst, and so it reads throughout this document. What the app does does not change.

2. Terms

These terms are normative. Every idea has one word; that word means exactly this throughout this document. The code is the name in the source code. In running text the terms are in lower case; only the names Customer portal, Office and Exact Online have a capital. The terms are in the order in which a customer meets them.

Term	Code	Meaning
Installation company	`InstallationCompany`	The client: the company that has the app built and uses it. It installs and maintains heat pumps and ventilation at businesses and schools.
Customer portal	`CustomerPortal`	The app for customers, at the address below.
Office	`Office`	The app for employees, at the address below. Only the app has this name (see below).
Relation	`Relation`	A business or school the installation company works for: an account in Exact Online, with a

		relation code, with at least one sales order. A supplier is not a relation.
Contact	`Contact`	A person at a relation in Exact Online, with a name and e-mail address.
Customer	`Customer`	Role: whoever signs in to the Customer portal with an e-mail address. One customer is one e-mail address, held by one or more contacts (GEG-003).
Employee	`Employee`	A person of the installation company with access to Office, with the role office employee or administrator.
Office employee	`OfficeEmployee`	Role: an employee who answers questions.
Administrator	`Administrator`	Role: the employee who invites employees in Organisation management, and blocks and restores the access of customers.
Sign-in link	`SignInLink`	A link by e-mail with which a customer signs in, without a password, in the browser that requested it (BEV-002).
Sign-in code	`SignInCode`	The code in the same e-mail as the sign-in link, to enter in the browser that requested the link (BEV-002).
Passkey	`Passkey`	What an employee signs in with and confirms an administrator's action with (BEV-006, ROL-010).

Sync	`Sync`	Reading the changes from Exact Online (KOP-004).
Order	`Order`	A sales order of a relation in Exact Online, with its order number and description.
Status	`OrderStatus`	The one text that says where an order stands, according to STAT-001. An order always has exactly one.
Planned date	`PlannedDate`	The delivery date of an order in Exact Online (`DeliveryDate`), shown as STAT-002 says.
Status change	`StatusChange`	A change of `Status` or `DeliveryDate` of an order in Exact Online, as the app saw it at a sync (VAST-002).
Order file	`OrderFile`	A document with an order in Exact Online: a work order, an invoice or another document, with one or more attachments.
Document type	`DocumentType`	The type of a document in Exact Online.
Kind	`FileKind`	What an order file is: work order, invoice or document. The kind follows from the document type (GEG-006).
Work order	`WorkOrder`	An order file with the report of work on an order.
Invoice	`Invoice`	An order file with the bill for an order.
Document	`OtherDocument`	Any other order file with an order, such as a

		completion report or certificate.
Attachment	`Attachment`	A file of an order file, such as a PDF, that opens.
Conversation	`Conversation`	The questions and answers with one order.
Question	`Question`	A text message from a customer about one order.
Answer	`Answer`	A text message from an office employee in the conversation of one order.
Open question	`OpenQuestion`	A question after which no answer has yet come in the conversation and that has not been closed.
Close	`Close`	Handling an open question without an answer. The question is then closed, and the customer receives no e-mail.
Access	`Access`	Whether a customer can sign in at a relation: Can sign in or Blocked.
Block	`Block`	Ending the access of an e-mail address at one relation. The result is a block (GEG-010).
Restore access	`RestoreAccess`	Lifting a block, so that the customer can sign in at that relation again.
Event	`Event`	Something the app counts per day for a measure of Core process (MEET-001).
Step	`Step`	One tap or click with which the user moves on. Typing in a field and scrolling are not a step.

Office is only the name of the app. The people who answer questions in it are office employees.

The addresses of the two apps:

- Customer portal: `https://portal.voorbeeld.example`
- Office: `https://office.voorbeeld.example`

The words Texts and images, Management area, Organisation management, Preview, Mobile, Tablet and Desktop mean what the Appwinst specification says (ADD-006, PRV-007).

3. Invariants

- **INVAR-001** A customer MUST be able to see or open only orders, order files and questions of their own relation. The server MUST check this on every request, also when an attachment is opened; a request for something of another relation gets the same response as a request for something that does not exist (ROL-009, SCH-005).
- **INVAR-002** The app MUST NOT write anything to Exact Online: the code that calls Exact Online can make only GET requests (KOP-001), even if the app's registration in Exact Online grants write permissions.
- **INVAR-003** A customer MUST be able to sign in and stay signed in only while they have access (GEG-003). The server MUST check this on every request, so that the end of access (ROL-007) also ends a session that was already open.
- **INVAR-004** Every order MUST have exactly one status, which STAT-001 gives. A status MUST NOT be empty, and an order MUST NOT show two statuses at once (STAT-003).
- **INVAR-005** What a screen shows from Exact Online MUST lag behind Exact Online by at most one sync (KOP-004). If the app cannot achieve that, the screen MUST show the last known data with the time at which it was updated (SCH-004, KOP-009), and MUST NOT show an empty list in place of data the app could not read.
- **INVAR-006** A question MUST belong to exactly one order, and to the customer who asked it for as long as that customer exists (GEG-011). A question MUST NOT move to another order.
- **INVAR-007** With every answer, every customer that MEL-005 names MUST receive exactly one e-mail, even if sending is retried (GEG-012).

4. Roles and permissions

The app has three roles across two portals: the customer on the Customer portal, the office employee and the administrator on Office. What ROL-004 does not allow, the app refuses.

- **ROL-001 Denied by default.** The app MUST refuse every action and every request for data that ROL-004 does not give to the role of the signed-in person. Identity, role and relation MUST come from the

session on the server, on every request, and never from what the browser sends along.

- **ROL-002 Customer.** A customer is a contact in Exact Online with an e-mail address, at a relation that has at least one sales order in the connected administration (VKL-003, GEG-002). They sign in only to the Customer portal, and have access to such a relation as long as the administrator does not block them there (GEG-003). There is no invitation and no account to create: access follows Exact Online. A contact of an account without a sales order, such as a supplier, is not a customer.
- **ROL-003 Office employee and administrator.** An office employee signs in only to Office, after an invitation from the administrator through Organisation management (ADD-006, I3). The administrator has every permission of the office employee, and in addition the permissions that ROL-004 gives only to them.
- **ROL-004 Permissions per role.** Each role has exactly the permissions below, and no others.

Customer. May: see orders and an order, with the status and the planned date, of their own relation (ROL-005); open an order file with an order (a work order, invoice or document) of their own relation, visible order files only (ROL-006); ask a question about an order of their own relation; read questions and answers with an order of their own relation. May not: answer a question or close an open question; see Customers; block or restore the access of a customer; invite employees, give them their role or remove them; change Texts and images or the settings in the Management area; write anything to Exact Online (BUITEN-001).

Office employee. May: see only the order with a question, with the status and the planned date; open an order file with an order that has a question, visible order files only (ROL-006); read the questions and answers with every order; answer every question and close every open question; see Customers: contact, relation and access. May not: ask a question; block or restore the access of a customer; invite employees, give them their role or remove them; change Texts and images or the settings in the Management area; write anything to Exact Online (BUITEN-001).

Administrator. May: everything the office employee may; in addition block and restore the access of a customer at a relation; invite employees, give them their role and remove them (Organisation management); change Texts and images, and the settings in the Management area, including the document types per kind (ROL-006) and the integration with Exact Online (KOP-009). May not: ask a question; write anything to Exact Online (BUITEN-001).

- **ROL-005 Own relation.** A customer's relation is the relation in Exact Online at which their contact is listed. An order belongs to exactly one

relation, read from one field of the sales order in Exact Online (**VRAAG-ROL-1**: does the orderer, the delivery address or the invoice address count?). That field decides who sees which orders; the installation company therefore answers the question before signing (BB-006), and the answer goes into this requirement. On Day 0 the Builder checks only that the chosen field is filled in the test administration (BOUW-002). An order MUST NOT become visible through a second field. If one e-mail address is held by contacts of more than one relation, that person is a customer of each of those relations; every request for data then applies to one of those relations at a time, and never to a relation of which they are not a contact (SCH-023).

- **ROL-006 Visible order files.** An order file is visible, to customers and employees, only if the table Document types per kind (GEG-006) gives its document type in Exact Online a kind (work order, invoice or document), and if the relation that Exact Online names with the document, where it is given, is the same as the relation of the order. A document type that the table does not name or marks not visible, the app shows to no one: Exact Online can also keep internal order files with an order. The table is empty until the installation company settles it with the Builder before Start (**VRAAG-ROL-2**: which document types in Exact Online are the work order, the invoice and the documents that customers may see?; BOUW-002); the administrator changes it after that in the Management area.
- **ROL-007 End of access.** A customer's access to a relation MUST end, also in a session that is already open: at their next request after the administrator blocks them at that relation; and at the next sync (KOP-004) in which no contact of that relation has their e-mail address any more, or in which the relation is no longer in the administration or no longer has a sales order. A block rests on the normalised e-mail address at one relation (GEG-010). It MUST remain in force if that address disappears from Exact Online and later returns, and ends only when the administrator restores access or the relation disappears. A block at one relation does not affect access to another relation. An employee whom the administrator removes in Organisation management loses access at their next request.
- **ROL-008 Separate portals.** A session of the Customer portal MUST NOT be valid on Office, and the other way round. A customer cannot sign in to Office.
- **ROL-009 Not found is not found.** A request for an order, order file or question outside the permissions of ROL-004 MUST get the same response as a request for something that does not exist (SCH-005). An address in the app SHOULD carry its own random key, not the order number from Exact Online.

- **ROL-010 Confirming with a passkey.** Blocking, restoring access, inviting an employee, inviting again (BEV-006), changing their role or removing them, changing the document types per kind and making the integration with Exact Online again MUST ask for a confirmation with the administrator's passkey within the last 10 minutes.

5. Domain model

Exact Online is the source of relations, contacts, orders and order files. The app keeps a copy of them that only the integration writes (BUITEN-001), so that a list does not have to ask Exact Online on every view and the app sees when a status changes. What users enter themselves (questions, answers, closures, blocks, the document types) belongs to the app. Every value is on one of the framework's two wires: YSQL (relational, with transactions, keys and constraints) or YCQL (on one key, with expiry and counters).

Entities

The name of each entity is the name in the model; where Terms also defines the word, it means the same. Per entity: identifier, what it belongs to, fields, source, and the wire with the reason.

- **Relation.** Identifier: the account ID of Exact Online (GUID); the relation code (`Code`) is unique. Belongs to: has contacts and orders. Fields: relation code, name. Source: the integration (`crm/Accounts`). Wire: YSQL: every access check goes through the relation; the relation code is unique through an index.
- **Contact.** Identifier: the contact ID of Exact Online (GUID). Belongs to: exactly one relation; exactly one customer, through the e-mail address. Fields: name (`FullName`), e-mail address (the field of IMP-003). Source: the integration (`crm/Contacts`). Wire: YSQL: key to relation and customer; listed per relation and searched in Customers.
- **Customer.** Identifier: a UUIDv5 of the normalised e-mail address; the address is unique. Belongs to: one or more contacts. Fields: e-mail address. Source: derived from the contacts. Wire: YSQL: signing in looks up the address; a question carries its identifier.
- **Block.** Identifier: the normalised e-mail address and the relation together. Belongs to: one e-mail address, one relation. Fields: blocked by (employee), blocked at. Source: what the administrator enters (Customers). Wire: YSQL: a block applies at once; the access check reads it in the same transaction; it does not refer to the customer, so that it remains if the customer disappears.
- **Order.** Identifier: the order ID of Exact Online (GUID); the order number is unique. Belongs to: exactly one relation; has order files, status changes and one conversation. Fields: order number, description, order date (`OrderDate`), planned date (`DeliveryDate`), `Status`. Source: the integration

(`SalesOrders`). Wire: YSQL: listed per relation by status and date; key for order files, status changes and the conversation.

- **Document type.** Identifier: the document type of Exact Online. Belongs to: nothing. Fields: name in Exact Online, kind (work order, invoice, document) or not visible. Source: settled before the Start (BOUW-002), after that the administrator (Management area). Wire: YSQL: every order file row of the integration reads it; a change starts a new reading of the documents.
- **Order file.** Identifier: the document ID of Exact Online (GUID). Belongs to: exactly one order; exactly one document type; has attachments. Fields: subject, date. Source: the integration (`Documents`). Wire: YSQL: listed per order; access follows the relation of the order.
- **Attachment.** Identifier: the attachment ID of Exact Online (GUID). Belongs to: exactly one order file. Fields: file name, file type, size. Source: the integration (`DocumentAttachments`). Wire: YSQL: only the reference; the app does not keep the content (GEG-007).
- **Status change.** Identifier: order, moment seen and field together. Belongs to: exactly one order. Fields: field (`Status` or `DeliveryDate`), old value, new value, seen at, changed in Exact (`Modified`). Source: the integration, at every sync. Wire: YSQL: written in the same transaction as the order that shows it, and deleted with the order.
- **Question, Answer.** Identifier: the message ID of the threads kit of Messages (A5). Belongs to: the conversation of exactly one order; a question from a customer, an answer from an office employee. Fields: text, written at, written by; for an answer also seen at. Source: what users enter (Order, Question). Wire: YSQL: the list of open questions filters across all orders, and the e-mail goes through the outbox in the same transaction.
- **Closure.** Identifier: the conversation and the moment together. Belongs to: the conversation of exactly one order. Fields: closed by (employee), closed at. Source: what an office employee enters (Question). Wire: YSQL: closes the open questions of that conversation in the same transaction.
- **Sign-in link.** Identifier: the customer identifier: at most one valid link per customer. Belongs to: exactly one customer. Fields: hash of the token, hash of the sign-in code, binding to the browser that requested it, failed attempts, used. Source: the app, on a request (Customer portal: Sign in). Wire: YCQL: expires on the clock (an expiry at write time, BEV-002), read on one key; use and failed attempts are conditional writes on that key; a new request overwrites the previous link.
- **Count.** Identifier: event and day together. Belongs to: nothing: no person, no relation, no order. Fields: number. Source: the app, at every event of Core process (MEET-001). Wire: YCQL: a counter, only incremented and read per event across days.

- **Sync.** Identifier: the source in Exact Online (relations, contacts, orders, documents). Belongs to: nothing. Fields: cursor, last succeeded at, last error. Source: the integration. Wire: YSQL: the cursor moves in the same transaction as the data it read; Orders, Order, Customers and the Management area read from it the time of the data (KOP-009).
- **Integration lock.** Identifier: the administration of Exact Online. Belongs to: nothing. Fields: version of the secret in the secret store, access token expires at. Source: the integration. Wire: YSQL: one row, locked with `SELECT ... FOR UPDATE` on every refresh, so that two never run at once (KOP-006). No token: that is in the secret store and in memory (BEV-009).

Employees (office employees and the administrator), their e-mail address, their role and their passkeys belong to Organisation management (ADD-006, BEV-006); this model refers to them by their identifier. The limits of BEV-004 per IP address, per e-mail address and for opened order files the server counts in its memory (AVG-003); questions per customer per day it counts from the questions themselves.

Requirements

- **GEG-001 Exact Online is the source.** Relation, contact, order, order file and attachment MUST be written only by the integration. No screen changes a value that comes from Exact Online; a change happens in Exact Online and reaches the app at the next sync (VKL-002). The integration reads only the fields of the entities above, with the keys and change moments the sync needs, and the field of ROL-005 (KOP-002, KOP-004).
- **GEG-002 Only what a step needs.** The app MUST keep a relation only if Exact Online has at least one sales order of that relation (VKL-003), and a contact only if they have an e-mail address and belong to a kept relation (AVG-004). Of a contact the app MUST read only name and e-mail address; the phone number, the job title and every other field MUST NOT be read or kept (BUITEN-008). Of an order the name of whoever changed it in Exact Online (`ModifierFullName`) MUST NOT be read, nor `DeliveryStatus` and `InvoiceStatus` as long as STAT-001 does not use them (OPEN-001); if OPEN-001 puts them in STAT-001, they join the fields of Order.
- **GEG-003 A customer is one e-mail address.** The app MUST keep one customer per e-mail address, normalised without spaces and in lower case, as long as at least one contact has that address. If two contacts with the same address are in Exact Online (a shared mailbox, or the same person at two relations), that is one customer with each of those relations (SCH-023). A customer has access to a relation if a contact of that relation has their address and there is no block of that address at that relation; Roles and permissions says what that access allows.

- **GEG-004 Identifiers that converge.** Relation, contact, order, order file and attachment MUST have the identifier of Exact Online as key, and a customer the UUIDv5 of their address, so that the same address always gives the same customer identifier. Every write of the integration MUST be an upsert on that key, so that a sync that runs again or reads a page again gives the same result. Every identifier is its own type, never a bare text or UUID.
- **GEG-005 Order, relation and order files.** An order MUST belong to the relation in the field that ROL-005 names; this model does not choose that field. A document in Exact Online is an order file of an order if it carries that order's order number (`SalesOrderNumber`) or is linked to the order itself (`SalesOrders.Document`); a document that belongs to the same order in both ways MUST be one order file. If Exact Online names with the document a relation (`Account`) that is not that of the order, the app MUST NOT keep it (ROL-006).
- **GEG-006 The document type decides the kind.** The app MUST keep a document as an order file only if its document type has a kind: work order, invoice or document. A document type that the app does not know, or that is not visible, MUST NOT be kept, not for Office either (ROL-006): Exact Online also keeps internal order files with an order. Until the Builder and the installation company settle the kind of each document type (BOUW-002, VRAAG-ROL-2), no document type has a kind. After that the administrator changes them in the Management area (ROL-004, ROL-010). After a change the integration reads the documents again, so that what becomes visible appears and what is no longer visible disappears. Whether the invoice with an order is in Exact Online as a document is VRAAG-KOP-2.
- **GEG-007 Attachments are passed on, not kept.** The app MUST NOT keep the content of an attachment. When a customer or employee opens an attachment, the integration fetches it from Exact Online and passes it on (KOP-005). Work orders and documents contain names and addresses; this way that content is in one place, and there is no second copy that must stay equal to Exact Online. Of the attachment the app keeps only name, type and size, for SCH-031 and the limit of KOP-005.
- **GEG-008 The status is derived, not kept.** The app MUST keep `Status` and `DeliveryDate` as Exact Online gives them, and derive the status from them on every view (STAT-001). The derived status MUST NOT be stored: a change of STAT-001 then applies at once to every order.
- **GEG-009 Questions, answers and closing.** Every order has at most one conversation. A question is written by a customer with access to the relation of the order, an answer by an office employee; the text is plain text (BUITEN-007, BEV-007), not empty and not longer than BEV-004

allows. A sent question or a sent answer MUST NOT be changed or deleted by a user (VRG-004). A question is open until an answer follows in the same conversation or an office employee closes the conversation (VRG-002). An answer is seen at the moment a customer of that relation first opens the order after it arrived (SCH-021); who that was, the app does not record. The conversation has a sequence number that rises with every message and every closure; an answer or closure names the sequence number the employee saw, and if something has been added in the meantime, the app MUST refuse it and show what was added (SCH-064).

- **GEG-010 A block remains until access is restored.** A block MUST apply to one normalised e-mail address at one relation, and MUST NOT change through a sync. If the address disappears from Exact Online and later returns at a contact of that relation, the block applies again (ROL-007). It ends only through restore access, or if its relation disappears from the app.
- **GEG-011 What disappears from Exact Online disappears from the app.** If a relation, contact, order, order file or attachment disappears from Exact Online, the app MUST delete it at the sync that sees this, at the latest at the full reading of the night (KOP-004). If no contact has a customer's address any more, the app deletes that customer with their sign-in link; their questions remain with their order, with deleted contact as sender, and the blocks of their address remain (GEG-010). With an order its order files, attachments, status changes and conversation disappear; with a relation its blocks.
- **GEG-012 Writing in one transaction.** Every write that touches more than one row MUST happen in one serializable transaction: a page of the integration with its status changes and the cursor of Sync; a question or answer with its e-mail in the outbox (INVAR-007); a closure with the end of the open questions; a block or the restoring of access with the record; a change of a document type with the record. An e-mail goes out only after the transaction has been committed. A transaction that hits a conflict runs again and gives the same result.
- **GEG-013 The read paths.** Every table serves at least one of these read paths, and every read path has its index:

Read path	Who	Key and order
A customer by their address	Customer portal: Sign in	unique on the e-mail address
The relations of a customer, without blocked ones	every request of a customer (INVAR-003)	contacts per customer, blocks per e-mail address and relation

The orders of a relation, ongoing by planned date and earlier newest first, per page	Customer portal: Orders	per relation, by `Status`, planned date and order date
An order by order number or description, within one relation	Customer portal: Orders (search)	within the orders of that relation
Orders with an answer not yet seen	Customer portal: Orders (New answer)	answers per order without seen at
One order with its order files and attachments	Customer portal: Order, Office: Question	order files per order, attachments per order file
The status changes of an order, newest first	Office: Question (SCH-061)	per order, by moment seen descending
The conversation of an order	Customer portal: Order, Office: Question	per order, in order of writing
The open questions, oldest first, and their number	Office: Questions	by the moment of the oldest open question
Answered and closed questions, newest first	Office: Questions	by the moment of the last answer or the closure
Relations with their contacts and blocks, and search by name, relation or e-mail address	Office: Customers	relations by name, contacts per relation; search reads the contacts, a few thousand rows (GEG-014)
An order by its order number	the integration, for GEG-005	unique on the order number
The document types	the integration, the Management area	by document type
The sign-in link of a customer	Customer portal: Sign in	the customer identifier
The counts of an event over a range of days	the measures of Core process	per event, by day descending

– **GEG-014 The scale.** The model holds about 1,200 customers, 5 office employees and 1 administrator, together 1,206 people (AAN-011, the Build request). The number of relations is at most the number of contacts. How many orders a relation has and how many order files an order, the Build request does not say: that is an open point for Day 0, which a count in the installation company's administration answers (BOUW-002). The model does not depend on it: every read path of GEG-013 is one indexed read per key, per page, except the search in

Customers, which at this size reads all contacts; and no key starts with an ascending value, so that the copy grows along with Exact Online without a different design.

- **GEG-015 Test data in the Preview, production from Live.** The Preview MUST read only the installation company's test administration (PRIV-005, INV-008, KOP-011). At Live the integration builds the copy from the administration in production; nothing from the Preview goes along, not the document types either: the administrator settles those for the production administration, with the table from the test administration as a proposal. The first state the app sees of an order is not a status change (BUITEN-004).

6. Core process

The core process is: **a customer sees for themselves how their order stands, with the work orders, the invoice and the documents with it.** The questions about an order and their answers are the Messages add-on in this Build.

The steps

The steps are those of the Build request, in this order and with these numbers, in the words of Terms.

- **PROC-001** The customer signs in. Screen: Customer portal: Sign in. Journey: REIS-001.
- **PROC-002** They see the orders of their relation with their status. Screen: Customer portal: Orders. Journey: REIS-002.
- **PROC-003** They open an order, with the work orders, the invoice and the documents with it. Screen: Customer portal: Order. Journey: REIS-003.
- **PROC-004** They ask a question about the order. Screen: Customer portal: Order. Journey: REIS-004.
- **PROC-005** An office employee answers and the customer receives an e-mail. Screens: Office: Questions and Office: Question. Journey: REIS-005. Notification: MEL-005.
- **PROC-006** The customer chooses a time for the annual maintenance. This step is not in this Build (BUITEN-003).

The order

- **STAT-001** The app MUST give each order exactly one status, from this table. A value that is not in the table gives In progress; the app MUST then record that value for Maintenance.

Status	Code	From Exact Online (`SalesOrders`)
Planned	`Planned`	`Status` 12 (Open) with a `DeliveryDate` of today or later

In progress	`InProgress`	`Status` 12 (Open) in every other case: without a `DeliveryDate`, or with a `DeliveryDate` before today; and every value that is not in this table
Partly delivered	`PartlyDelivered`	`Status` 20 (Partial)
Completed	`Done`	`Status` 21 (Complete)
Cancelled	`Cancelled`	`Status` 45 (Cancelled)

- **STAT-002** The app MUST show the planned date with the status Planned and with Partly delivered with a `DeliveryDate` of today or later, and nowhere else. A date that has passed no longer promises anything.
- **STAT-003** The app MUST NOT show a second status beside the one, and MUST NOT show an empty status such as "Status not available" ([22], [21]).
- **STAT-004** Current are the orders with In progress, Planned or Partly delivered; Earlier are the orders with Completed or Cancelled.
- **OPEN-001** Question to the installation company, before signing. Which values `DeliveryStatus` and `InvoiceStatus` have is not in the research basis. STAT-001 therefore does not use them. If a value of either must change the status, for example to a status for a delivered or invoiced order, that is written into STAT-001 before signing.

The question

- **VRG-001** The conversation of an order is shown with that order, in the order in which the messages were sent, each with its time. A question shows the name of the customer; in the Customer portal an answer shows the name of the installation company.
- **VRG-002** A question is open until an office employee answers it or closes it. A new question on that order is again an open question. With each question the customer sees whether it is open, answered or closed.
- **VRG-003** Every customer of the relation sees the conversation on the orders of that relation. A customer of another relation never sees it.
- **VRG-004** A question or answer cannot be changed or deleted once sent. A correction is a new message.

Journeys, outcomes and measures

Each journey earns an outcome for the installation company. The app measures what happens in the app, with the event for each measure. The installation company measures the number of phone calls itself. The numbers in brackets are those of the Research basis.

REIS-001 Sign in

- App and role: Customer portal, customer.

- Outcome: in without a password.
- Measure and event: the share of sent sign-in links that leads to a session: `inloglink_verstuurd`, `inloglink_gebruikt`.
- Pattern and source: signing in without a password with a link by e-mail, for accounts that are rarely used; one field, one button ([23], [20]).
- Done path: KLAAR-001.

REIS-002 Where is my order?

- App and role: Customer portal, customer.
- Outcome: the state found without calling.
- Measure and event: the share of sessions that opens an order: `sessie_gestart`, `order_bekeken`. Outside the app: phone calls per day, against the 40 of the Build request.
- Pattern and source: one status per order with the planned date, current orders at the top ([24], [20], [22]).
- Done path: KLAAR-006.

REIS-003 Need a work order or invoice

- App and role: Customer portal, customer.
- Outcome: the order file opened by the customer, not asked for again.
- Measure and event: opened attachments per kind: `werkbon_geopend`, `factuur_geopend`, `document_geopend`.
- Pattern and source: the order files with the order itself, not in separate lists ([26]; [25], marketing and therefore weighted lightly).
- Done path: KLAAR-010.

REIS-004 A question about an order

- App and role: Customer portal, customer.
- Outcome: the question in writing with the order, no phone call.
- Measure and event: questions per viewed order: `vraag_gesteld`, `order_bekeken`; answers read: `antwoord_gelezen`.
- Pattern and source: a contact channel in the overview per job, as the peers show it ([25]); uncertainty about an order drives contact ([20], [22]). The evidence for this form is thin.
- Done path: KLAAR-015.

REIS-005 Answer a question

- App and role: Office, office employee.
- Outcome: one answer with the order beside it, and the customer is notified.
- Measure and event: the time to the first answer (median) and the open questions at the end of the day, read from the questions and answers themselves (VAST-001); `vraag_beantwoord`, `vraag_afgesloten`.
- Pattern and source: one work list with the oldest open question at the top; e-mail only for a new answer, with a direct link (the research for the Fit

check, §3 pattern 5, evidence thin; the order is a design choice to limit the waiting time, without a source).

- Done path: KLAAR-023.

REIS-006 Manage access

- App and role: Office, administrator.
- Outcome: only the right people can get in.
- Measure and event: no commercial measure: `toegang_geblokkeerd`, `toegang_teruggezet`.
- Pattern and source: access follows the contacts in Exact Online (VKL-003); blocking asks for a confirmation with the passkey (ROL-010). No source in the research basis.
- Done path: KLAAR-029.

The six steps of the Build request are the steps PROC-001 to PROC-006, not six phases of an order: the order shows one status from Exact Online (STAT-001), not a timeline.

Measuring

- **MEET-001** The app MUST count each event of the journeys per day, without a person, relation or order, as VAST-003 says; the kind of an order file is only in the name of the event. An event that counts per session (`sessie_gestart`, `order_bekeken`) counts as VAST-003 settles it for a session.
- **MEET-002** The app MUST NOT use third-party analytics or tracking cookies. The installation company reads the measures from the counts and from the questions and answers, in the export of its data (BEH-011).

7. Screens

- **SCH-001** The Build has seven screens in two portals. The Customer portal has Sign in, Orders and Order. Office has Sign in, Questions, Question and Customers. Texts and images, Management area and Organisation management are in every Build and do not count (ADD-006).
- **SCH-002** The Customer portal is designed Mobile first, Office Desktop first. Every screen works on Mobile, Tablet and Desktop.
- **SCH-003** Every screen opens with its own heading, shows one main action and says where the user can go next. Every empty state says what is there, what the area is for, and offers one action.
- **SCH-004** If Exact Online cannot be reached, or the integration does not work (KOP-009), every screen with data from Exact Online MUST show the last known data, with the time at which it was updated, and say that it is not current. It MUST NOT show an empty list or only an error message as if there were nothing.
- **SCH-005** An order, order file or question that does not exist or does not belong to the user gives the same "Not found" page. The page does not say which of the two it is (ROL-009).

Customer portal: Sign in

- **SCH-010** Shows one field for the e-mail address and one button to send a sign-in link. The field lets the browser fill in the e-mail address.
- **SCH-011** After sending, the screen says, the same for every address: if the address has access, a sign-in link is in the mailbox (BEV-003). Below it is a field for the sign-in code from that e-mail, for those who open the e-mail on another device or in another browser.
- **SCH-012** A sign-in link or a correct sign-in code opens Orders, or the page the customer had to sign in for, such as the order from an e-mail.
- **SCH-013** States: empty field or no valid e-mail address (the screen says what is missing and keeps the input); link sent, with the field for the sign-in code; sign-in code incorrect (the screen says so, and keeps the input); an incorrect sign-in code too often, or too many requests (the screen says that a new link is needed, and when that is possible again, BEV-002, BEV-004); link used or expired (a page that says so, with one button for a new link); session expired (this screen, with the page the customer was on as the destination).
- **SCH-014** If a customer opens the sign-in link in a different browser from the one that requested it, a page says that the link only works in the browser in which they requested it, and that they can enter the sign-in code from the e-mail there. That page MUST NOT show the sign-in code.

Source: the contacts with their e-mail address from the integration with Exact Online, and the blocks the administrator enters.

Customer portal: Orders

- **SCH-020** Shows the orders of the customer's relation, first Current, then Earlier (STAT-004). Current orders are sorted by planned date, the first at the top, and orders without a shown date after them; earlier orders are newest first. A relation always has at least one order, because otherwise it is not a relation and no one can sign in with it (ROL-002, ROL-007).
- **SCH-021** Each order shows order number, description, status (STAT-001) and the planned date where STAT-002 shows it. An order with an answer that no customer of the relation has opened yet carries the label New answer (GEG-009).
- **SCH-022** A search field finds an order by order number or description.
- **SCH-023** If the customer's e-mail address is with more than one relation, they choose the relation above the list, and the list shows only its orders. With one relation there is no choice.
- **SCH-024** States: loading; no current orders (in the place of Current the screen says that there is no current order now, that a new order appears here once it is in Exact Online, and how the customer reaches the installation company, from Texts and images; the earlier orders are

below it); no search result (with a button to clear the search); Exact Online cannot be reached (SCH-004).

Source: the integration with Exact Online (orders, status, planned date); the answers that office employees enter (the label New answer).

Customer portal: Order

- **SCH-030** Shows at the top order number, description, status and planned date (STAT-001, STAT-002), below that the order date and, with more than one relation, the name of the relation. On Mobile there is a link below the status to the field for a question.
- **SCH-031** Shows the order files of the order in three groups, in this order: work orders, invoice, documents. Each group is always there; a group without order files says that there are none yet. Each order file shows subject and date, and each attachment of the order file is on its own line with its file type and size; each attachment opens in one step. Only order files whose document type has a kind are included (GEG-006, ROL-006).
- **SCH-032** Shows the conversation of the order (VRG-001, VRG-002), with below it a field for a question and one button to send it. After sending, the question is at the bottom at once, with its time, and the screen says that the customer will receive an e-mail when there is an answer.
- **SCH-033** States: loading; an order without order files (each group says that there is nothing yet, and the field for a question is below); an attachment that cannot be opened now, also when it is too large or the daily budget is used up (the screen says so, at that attachment, and the rest stays usable, KOP-005, KOP-007); empty question field (the button sends nothing and the screen says what is missing); a question that is too long (the screen says how many characters are allowed, and the text stays, GEG-009); too many questions in a day (the screen says so, and the text stays, BEV-004); sending failed (the text stays, with a button to send again); Exact Online cannot be reached (SCH-004); not found (SCH-005).

Which document types are a work order, an invoice or a document is settled by GEG-006 and ROL-006 (VRAAG-ROL-2).

Source: the integration with Exact Online (the order, its status and its order files with their attachments); the questions that customers enter and the answers that office employees enter.

Office: Sign in

- **SCH-040** Shows one button to sign in with a passkey (BEV-006). There is no field for a password or an e-mail address, and Office sends no sign-in link. Below the button, for those who have no passkey on this device: a passkey that one's own password manager syncs works on

every device; otherwise they ask the administrator for a new invitation in Organisation management.
- **SCH-041** Only an employee can sign in here. A customer cannot sign in here (ROL-008).
- **SCH-042** After signing in, Questions opens, or the page the employee had to sign in for, such as the question from an e-mail (BEV-014).
- **SCH-043** States: sign-in cancelled or refused (the screen says so, with the button to try again and the explanation of SCH-040 for those who have no passkey); the administrator's first sign-in with one passkey (the screen asks for a second passkey on another device, and they only go on once it is there, BEV-006); session expired (this screen, with the page the employee was on as the destination).

Source: the employees the administrator invites in Organisation management, with their passkey.

Office: Questions

- **SCH-050** Shows the orders with an open question, the oldest open question at the top. Each row shows relation, order number, name of the customer, the start of the question and since when it has been open.
- **SCH-051** A choice above the list shows the answered and closed questions instead, newest first, with who answered or closed them.
- **SCH-052** The navigation of Office shows the number of open questions beside Questions.
- **SCH-053** States: loading; no open questions (the screen says so, with the choice for answered and closed questions).

Source: the questions that customers enter and the answers that office employees enter; relation and order number from the integration with Exact Online.

Office: Question

- **SCH-060** Shows the conversation of one order (VRG-001), with the name of the office employee at each answer, and below it a field for an answer and one button to send it.
- **SCH-061** Shows the order as the customer sees it: status, planned date and order files (SCH-030, SCH-031). Below that the status changes of the order (VAST-002), newest first, each with the date on which the app saw it, the field and the old and the new value. On Desktop the order and the conversation are side by side; on Tablet and Mobile the conversation comes first.
- **SCH-062** Another button closes the open question without an answer (Close), after a confirmation.
- **SCH-063** After sending or closing, the screen says what happened and offers one button to the next open question, or to Questions if there are no more.

- **SCH-064** States: loading; empty answer field (the button sends nothing and the screen says what is missing); an answer that is too long (the screen says how many characters are allowed, and the text stays, GEG-009); a colleague answered or closed while the employee was typing (the screen shows that, the employee's own text stays, and sending then asks for confirmation); sending failed (the text stays, with a button to send again); not found (SCH-005).

Source: the questions that customers enter and the answers that office employees enter; the order, its order files and its status changes from the integration with Exact Online.

Office: Customers

- **SCH-070** Shows the relations from Exact Online with their contacts. Each contact shows name, e-mail address and access (Can sign in or Blocked); with Blocked also who blocked and when.
- **SCH-071** A search field finds a contact by name, relation or e-mail address.
- **SCH-072** With each contact with Can sign in there is a Block button for the administrator; with Blocked a Restore access button. A block applies to that e-mail address at that relation (GEG-010). Blocking asks for a confirmation that says the customer can then no longer sign in at that relation, even if their address is in Exact Online again later; the confirmation is the one with the passkey of ROL-010. After the confirmation the row shows the new access at once. An office employee sees neither button (ROL-004).
- **SCH-073** A contact that disappears from Exact Online, or no longer has an e-mail address, is no longer in Customers (GEG-002, GEG-011). Their block stays: if the address is with a contact of that relation again, their row shows Blocked.
- **SCH-074** States: loading; no search result (with a button to clear the search, and the explanation that a person is only here if they have an e-mail address in Exact Online at a relation with a sales order); Exact Online cannot be reached (SCH-004).

Source: the integration with Exact Online (relations and contacts with their e-mail address); the blocks the administrator enters.

8. Integration and import

Integration with Exact Online

The app has one integration: it reads from one administration in Exact Online and writes nothing to it.

- **KOP-001 One administration, read only.** The app MUST read from one administration of Exact Online, through the REST API (`/api/v1/{division}/…`): sales orders (`salesorder/SalesOrders`, with the sync variant `sync/SalesOrder/SalesOrderHeaders`), documents of an order (`documents/Documents`, through `SalesOrderNumber`, with the attachments through

`DocumentAttachments`), contacts (`crm/Contacts`) and relations (`crm/Accounts`) (Exact Online REST API, resource overview and the pages of SalesOrders, Documents and Contacts, undated). The code that calls Exact Online MUST only be able to make GET requests: any other request does not exist in the app (BUITEN-001).

- **KOP-002 Only the fields needed.** Each request MUST ask only for the fields the Domain model names. The app MUST NOT read `Phone`, `Mobile` or `ModifierFullName` (GEG-002, BUITEN-008).
- **KOP-003 Registration and scopes.** The main user of the installation company registers the app in the Exact App Center, in a subscription in the name of the installation company, with the scopes "Sales orders", "Organization documents" and "Crm accounts", and no others (Exact Online REST API, undated; Apideck, Exact Online configuration, undated). An app for one's own administration needs no review by Exact (Exact Knowledge Base, App publication procedure, undated; Apideck, undated). The client ID and the client secret come only through the secrets form (WK-003). The sources name no scope that allows reading only (**VRAAG-KOP-1**: does Exact Online offer a scope or a user role that allows reading only?); until there is one, KOP-001 makes the app read-only. The account in Exact Online that authorises the integration SHOULD only have rights to sales orders, documents and relations, because Exact Online also limits access to the rights of that user (Apideck, undated).
- **KOP-004 Syncing.** The app MUST read the changes every 5 minutes through the sync endpoints of sales orders, documents, contacts and relations, so that a change in Exact Online is in the app within 10 minutes (INVAR-005); and every night all contacts and relations through the bulk endpoints (1,000 records per page; Exact Online REST API, undated; Chift, undated). What is missing from that full read, the app deletes (GEG-011), and the access that relied on it ends (ROL-007). The app uses no webhooks: `Status` of a sales order has none (Exact Online REST API, SalesOrders, undated), a webhook does not say what changed, so that a GET follows anyway (Hookdeck, undated), and a webhook asks for the extra scope "Organization administration" and an address anyone on the internet can call. Every change of the status that a sync sees, the app records as Records and audit says (VAST-002, BUITEN-004).
- **KOP-005 Order files on request, attachments not kept.** The app MUST keep of an order file only the data the Domain model names, never the content of its Attachment (GEG-007). If someone opens an order file, the server checks ROL-004 and ROL-006, fetches the Attachment from Exact Online and passes it straight to the browser, up to 25 MB. So Exact Online stays the source (BUITEN-001, VKL-002), the app keeps

no copy of work orders and invoices with names and addresses (AVG-004), and no storage grows beyond the base of Maintenance (BEH-008).

- **KOP-006 Tokens.** The app MUST use OAuth 2.0 with the authorization code flow. An access token is valid for 10 minutes and can only be refreshed after 9 minutes and 30 seconds; refreshing earlier gives an error (Apideck; Nango; Hookdeck; Exact Knowledge Base, Get/use access tokens; all undated). The app refreshes it after that, and never at the same time as another refresh. A refresh token can be used once and expires after 30 days without use (Apideck; Exact Knowledge Base; Microsoft Power Users, "Old refresh token used"; all undated). The app MUST write each new refresh token to the secret store before it uses the new access token (BEV-009). If that fails, the sync stops and KOP-009 applies. The access token is only held in memory.
- **KOP-007 Limits.** Exact Online allows per app and per administration 60 calls per minute and 5,000 calls per day, and per administration a ceiling for all apps together: 20,000 calls per day on Essentials, Plus and Professional, 30,000 calls per day on Premium. Those are the limits that apply now, with the start date that [11] names ([11]; Barcode Scan, undated; Apideck, undated). Parallel calls are not allowed (Apideck, undated). The app MUST make one call at a time, follow the `X-RateLimit-Minutely-Remaining` headers (Peliqan, undated), wait until the next minute after a 429, and itself make no more than 4,000 calls per day, of which 1,500 calls per day stay free for KOP-004: four sync endpoints in each round of KOP-004 are 1,152 calls per day, and the nightly read needs a few. If the daily budget is used up, an order file no longer opens that day and Order says so at that order file (SCH-033); the sync goes on. The app does not use the XML API, because there one call counts as 50 ([11]).
- **KOP-008 Errors and timeouts.** After about 10 failed calls per hour Exact Online blocks an endpoint for the rest of the hour (Apideck; Exact Support, API rate limits; both undated). The app MUST NOT call an endpoint again for the rest of the hour after 3 failed calls per hour on that endpoint. Every call to Exact Online has a timeout of at most 30 seconds.
- **KOP-009 When Exact Online does not answer.** If Exact Online cannot be reached, or the integration no longer works, every screen with data from Exact Online MUST show the state of the last successful sync, with its time, and say that it is not current; it MUST NOT show an empty list as if there were no orders (SCH-004). The administrator receives an e-mail about it (Notifications) and sees the state of the integration in the Management area, where they set up the integration again (ROL-010).

The installation company can revoke the app in Exact Online at any time; then this applies too.

- **KOP-010 Test access before Day 0** (BC-005, WK-001 items 3 and 4). Exact Online has no sandbox (Apideck; Cyclr, Exact Setup; both undated). The installation company MUST put the test administration in a developer subscription of Exact Online, in its name and at its expense (VKL-005), not in a trial: a trial runs out while the Preview and every fix in the Bug window still need the test administration (INV-008, PRIV-005). The main user registers the app in that subscription (KOP-003), or grants the right "Manage apps" there (Genkgo, undated); the details come through the secrets form. A test administration does not prove that the installation company's own package has sales orders; the installation company confirms that before signing. Before Start the Builder checks in the test administration: (a) `SalesOrders` gives the test orders; (b) at least one order has a work order and an invoice as a document, found through `SalesOrderNumber`; (c) there are contacts with an e-mail address at a relation with a sales order. If any of the three fails, the Build is not ready to Start (WK-001).
- **KOP-011 Test and production separate.** The Preview MUST only read the test administration, with the details of the test registration (INV-008, GEG-015). The details for the production administration come through the secrets form at the moment Build plan by day names, and are only on the production server.

Open points, besides VRAAG-ROL-1 and VRAAG-ROL-2 (before signing) and VRAAG-KOP-1 (Day 0):

- **VRAAG-KOP-2** Does the invoice of an order come as a document through `Documents`, or only through another endpoint? Another endpoint may need an extra scope (KOP-003); the sources do not say.
- **VRAAG-KOP-3** Does a sync endpoint also report that a contact or relation was deleted? If not, the app only sees a deletion at the nightly full read (KOP-004, Security, residual risk 3).
- **VRAAG-KOP-4** Does fetching an attachment through `DocumentAttachments` count as one call? KOP-007 counts one call for it.
- **VRAAG-KOP-5** Which package does the installation company have: Essentials, Plus, Professional or Premium? The ceiling of the administration depends on it (KOP-007), and the app shares it with the installation company's other apps (VKL-005).

Import

- **IMP-001 No import file.** This Build imports no file (BUITEN-002). The roughly 1,200 contacts that the Build request named as a CSV export from Exact Online, with company, name, e-mail address and phone number, come through the integration with Exact Online, as a contact with its relation (Domain model).

- **IMP-002 Why not.** Appwinst imports only a clean file: one row per record, named columns, no cleaning by Appwinst (NIET-001, N4). Here clean also asks for a key per row that links the contact to its relation in Exact Online: the relation code. The CSV names only the company name, and linking a contact to a relation by name is cleaning (two relations with the same name, a name spelt differently). The integration reads the same contacts with the identifier of their relation, and keeps them current: whoever the installation company adds in Exact Online can sign in; whoever disappears no longer can (GEG-011). A one-off file does not do that.
- **IMP-003 Where each column of the CSV now comes from.**

Column in the CSV	In the app	Through
company	The relation of the contact	The identifier of its relation in Exact Online, not the name
name	The name of the contact	The integration
e-mail address	The e-mail address of the contact, and so the customer	The integration; which e-mail field of Exact Online, `Email` or `BusinessEmail`, is in Appendix: configuration values
phone number	Nothing	Not read (GEG-002, BUITEN-008)

- **IMP-004 Nothing to supply.** The installation company supplies no file on Day 0, and no one creates a customer in the app. A contact gets access only by being in Exact Online with an e-mail address at a relation with a sales order (VKL-003); the administrator can block that access (GEG-010).

9. Notifications

- **MEL-001** The app notifies only by e-mail (BUITEN-009).
- **MEL-002** The app MUST send every e-mail from an address on its own subdomain `mail.voorbeeld.example`, with SPF, DKIM and DMARC aligned on that domain, as COM-010 settles it for Appwinst. That subdomain accepts no mail (a null MX, RFC 7505), as Appwinst does for its own notifications (COM-011, the fallback in §27 of the Appwinst specification).
- **MEL-003** Every e-mail MUST contain a short summary and end with one link, with otherwise only the closing and the company details of the installation company; the e-mail with the sign-in link also contains the sign-in code (BEV-002). An e-mail MUST NOT contain the text of a question or answer, and MUST NOT carry an order file as an attachment (as COM-010).

- **MEL-004** Sign-in link. Whoever requests a link on Customer portal: Sign in for an address with access receives at once an e-mail with the sign-in link and the sign-in code. This e-mail is never delayed. Employees sign in with a passkey and receive no sign-in link (BEV-006).
- **MEL-005** New answer. When an office employee sends an answer, every customer with an open question on that order receives one e-mail with the order number and a link to the order.
- **MEL-006** New question. When a question is asked on an order without an open question, every office employee receives one e-mail with the order number, the relation and a link to Question. A further question on that order, while there is an open question, sends no e-mail.
- **MEL-007** A reply to an e-mail. The app receives no e-mail. A reply to an e-mail from the app comes back to the sender, because the subdomain accepts no mail (MEL-002), and its content never reaches the app. Whoever has a question follows the link with which every e-mail ends (MEL-003).
- **MEL-008** The app sends no e-mail other than those of MEL-004, MEL-005, MEL-006 and MEL-009. Closing (SCH-062), blocking and restoring access (SCH-072) send no e-mail.
- **MEL-009** The integration. If the sync with Exact Online no longer succeeds (KOP-009), the administrator receives one e-mail with a link to the Management area; if it succeeds again after that, they receive one that says so. Between those two no e-mail about the integration is sent.

10. Records and audit

The app records what a step, a measure or the accountability of an action needs, and no more. The installation company answered in the Build request that it does not need to show afterwards who changed what; this Build therefore has no Audit trail (BUITEN-012).

- **VAST-001 What the app records.** Per record: who or what makes it and when, where it sits in the Domain model, and how long it stays.

What	Who or what, and when	Where, and how long
A change of `Status` or `DeliveryDate` of an order	The integration, at the sync that sees it	Status change; as long as the order is in the app
A question: who wrote it and when	The customer who asks it, on sending	Question; VAST-007
An answer: who wrote it, when, and when a customer of the relation first saw it	The office employee, on sending; the seeing by the app, on the first opening of the order	Answer; VAST-007
A closing: who closed and when	The office employee, on closing	Closing; VAST-007

Blocking and restoring access: which e-mail address, at which relation, by whom, when	The administrator, at the action	Block, with a record per action; VAST-007
A change of a document type: which, from which kind to which, by whom, when	The administrator, at the action	Document type, with a record per action; as long as the app runs, the employee only by their identifier (VAST-004)
A requested sign-in link, and whether it was used	The app, on requesting and using	Sign-in link; VAST-007
How often each event of Core process occurs per day (MEET-001)	The app, at the event	Count; 13 months: enough to compare a year with the previous one; no personal data (VAST-003)
How many questions are open at the end of a day	The app, daily, at the end of the day	Count; as the other counts
When the integration last succeeded, and the last error	The integration, at each sync	Sync; only the last state
A value of `Status` that STAT-001 does not know, with the key of the order	The integration, at the sync that sees it	The server log (VAST-006); as the server log (PRIV-007)
Who changed a text or image	Texts and images, on publishing	That module (ADD-006); as that module keeps it
Who invited an employee, gave them a role or removed them	Organisation management, at the action	That module (ADD-006); as that module keeps it

- **VAST-002 Status history from Live.** Exact Online keeps only the current status of an order, not the history (Exact Online REST API, SalesOrderSalesOrders, undated). The app MUST therefore record each change it sees itself, from the first sync with the production administration (GEG-015, BUITEN-004), with the moment at which the app saw it and the moment Exact Online names as the last change. Office: Question shows them (SCH-061). The moment seen lies at most one sync after the change (KOP-004). A change that arises between two syncs and disappears again, the app does not see. Who changed the order in Exact Online, the app does not record (GEG-002).
- **VAST-003 Not recorded: who viewed what.** The app MUST NOT record which customer viewed which order or which attachment they opened, and an event of Core process MUST NOT carry a person,

relation or order. The measures of Core process are read by the app from Counts per event per day, and an order file that is opened counts per kind. A measure that counts per session counts at most one event per session. The time to the first answer the app reads from the questions and answers themselves. Of the reading, the app records only per answer when it was seen, without by whom (GEG-009, SCH-021). No step needs more (GDPR Art. 5(1)(c) and Art. 25 [27]).

- **VAST-004 Persons only by their identifier.** A record MUST name a person by their identifier, not by their name; the name comes on reading from the contact or from Organisation management. If a person disappears, the record stays, with deleted contact or deleted employee where the name was, as PRIV-009 settles it for Appwinst itself. The one exception is the block: it names the e-mail address, because it must keep applying if the address comes back (GEG-010).
- **VAST-005 No Audit trail.** The records are not chained to each other, and there is no separate export of them. The whole dataset of the app, records included, can be exported at any time (BEH-011). An audit trail with export is the Audit trail add-on (BUITEN-012).
- **VAST-006 No content in logs.** Server and access logs MUST NOT contain the text of a question or answer, a token, a sign-in code, a sign-in link, a name, an e-mail address or the content of an attachment (BEV-009). They and the backups follow the periods of PRIV-007.
- **VAST-007 Kept by purpose.** Each item of personal data stays as long as its purpose needs it (GDPR Art. 5(1)(e) [27]). This is the one place for those periods; AVG-003 names the purpose and refers here, and keeps only the periods of the IP address, the logs and the backups.

Data	Purpose	Kept
Name and e-mail address of a contact, and the customer	Signing in, and the questions of the relation	As long as they are in Exact Online; deleted at the sync that sees they are no longer there (GEG-011)
A block: the e-mail address, the relation, who blocked and when	Refusing access lastingly (ROL-007)	Until the administrator restores access, or until the relation disappears from the app (GEG-010)
A question or answer, with who and when, and a closing	Handling the question, and finding it again at a later question or the next annual maintenance	24 months after the last message or the last closing in the conversation of that order, or shorter if the order disappears from Exact Online (GEG-011)

A sign-in link	Signing in	Until it is used, lapses through a new request or expires (BEV-002)
Name, e-mail address and role of an employee	Signing in to Office, and with an answer	Until the administrator removes them in Organisation management
The content of an order file	Showing	Not kept (GEG-007)

The period for a conversation covers two rounds of the annual maintenance, so that an office employee finds a question about an order again at the next visit. After the period the app MUST delete the data: what GEG-011 names at the sync that sees it, and a conversation with its closings within a day after the end of its period, by a clean-up job. A deletion is final; the backups follow PRIV-007. These periods are in the data processing agreement (PRIV-007, the row Client app production data); another period is a new version of this document (ALG-005). If the service ends, BEH-012 applies.

11. Security

The app follows the Appwinst baseline for every client app (SEC-017) and tests both apps against OWASP ASVS 5.0, level 2 (Conformance). Every boundary an attacker touches is below with its threat model; beneath it, the requirements that close them.

Threat model by boundary

G1 Customer portal: a customer's browser and the server.

1. What an attacker wants: a relation's orders, order files and questions; a customer's session or sign-in link.
2. Who: a customer of another relation with a valid session; someone who is forwarded a sign-in e-mail or reads along in a mailbox; a bot that tries e-mail addresses; a former contact.
3. The boundary: inbound an e-mail address, a sign-in code, keys of orders, order files and questions, a destination after signing in, and the text of a question; outbound the data of the customer's own relation. At the boundary the server checks the session, the role and the relation (ROL-001), ownership for every item (ROL-004), the length of the input, the destination (BEV-014) and the origin of the request (BEV-001).
4. STRIDE: **S** a sign-in link signs in only in the browser that requested it (BEV-002). **T** a customer changes no data from Exact Online; the text of a question is shown as text (BEV-007). **R** who asked a question and when is recorded (Records and audit). **I** guessing a key gives nothing (ROL-009); whether an e-mail address is known does not leak (BEV-003). **D** sign-in requests, questions and opened order files per

customer are limited (BEV-004). **E** the browser carries no role; a Customer portal session is not valid in Office (ROL-008).

5. Abuse: a customer opens order files until Exact Online's daily budget is spent (BEV-004, KOP-007); someone keeps requesting sign-in links for another person's address (BEV-004); a question with a link to mislead an employee (BEV-007); a sign-in link with a destination on another site (BEV-014).
6. Invariant: no response of the Customer portal contains data of a relation the signed-in person has no access to at that moment.

G2 Office: an employee's browser and the server.

1. What an attacker wants: all questions and answers, the list of customers, lifting a block, the integration.
2. Who: a customer posing as an employee; an employee who has left; someone who phishes the administrator or reads along in an employee's mailbox.
3. The boundary: inbound answers, blocks, invitations and settings; outbound questions, orders with a question and customers. At the boundary the server checks the passkey session, the role (ROL-004) and, for the actions of ROL-010, a fresh confirmation.
4. STRIDE: **S** employees sign in with a passkey, which cannot be phished, and there is no fallback to a sign-in link (BEV-006). **T** an answer is shown as text (BEV-007). **R** who blocked, restored access, invited or answered, and when, is recorded (Records and audit). **I** an employee sees an order only with a question (ROL-004). **D** not applicable beyond BEV-004: there are five employees and no open registration. **E** an employee gets more rights only through Organisation management, with a passkey confirmation (ROL-010).
5. Abuse: an employee who leaves and still has an open session (ROL-007); an administrator who blocks someone by mistake (he restores access, ROL-004); someone posing as an employee who has lost his passkey, to get an invitation (only the administrator invites again, with his passkey; BEV-006).
6. Invariant: only an administrator with a passkey confirmation from the last 10 minutes changes a block, a role, an invitation, the document types by kind or the integration.

G3 The server and Exact Online.

1. What an attacker wants: the refresh token and the client secret, because with them he reads the whole administration within the scopes; a write action in Exact Online.
2. Who: whoever reads the server, a log or a backup; a forged or broken response; a bug in the app.

3. The boundary: outbound only GET requests with an access token; inbound orders, documents, contacts, relations and attachments. The server checks the host, the type and the size of every response.
4. STRIDE: **S** the app talks only over HTTPS to Exact Online's host, and fetches an address Exact Online returns only if it is on that host (BEV-010). **T** every response is checked for form and size (KOP-005, BEV-008). **R** not applicable: the app writes nothing in Exact Online (KOP-001). **I** tokens and secret are only in the secret store and in memory, never in the database or a log (BEV-009). **D** the budget, the timeout and the error limit keep Exact Online open (KOP-007, KOP-008). **E** only GET exists in the code (KOP-001), with the smallest set of scopes (KOP-003).
5. Abuse: a customer who uses up the administration's daily budget through many order files, also for the installation company's other apps (KOP-007, BEV-004); an address in a response that points to an internal service (BEV-010).
6. Invariant: the app sends Exact Online only GET requests, only to Exact Online's host, and the refresh token is only in the secret store.

G4 E-mail: the app and the mailbox.

1. What an attacker wants: a sign-in link; the content of a question or answer.
2. Who: someone who is forwarded an e-mail, reads along in a mailbox or poses as the sender.
3. The boundary: outbound a short notice with a link; inbound nothing. The sending domain accepts no e-mail (null MX, RFC 7505; MEL-002): a reply to an e-mail from the app goes back to its sender and never reaches the app (BEV-015).
4. STRIDE: **S** the app sends from its own subdomain with SPF, DKIM and DMARC (MEL-002). **T** not applicable: the app receives no e-mail, so there is no incoming content to forge, no automatic reply a forged sender can abuse and no loop with another automatic reply. **R** not applicable, for the same reason. **I** an e-mail contains no text of a question or answer, no order file and no attachment (BEV-011); what someone writes back never enters the app or its logs. **D** sign-in requests are limited (BEV-004). **E** a sign-in link gives no session in another browser (BEV-002), and an employee never signs in with an e-mail (BEV-006).
5. Abuse: using the app to send a lot of e-mail to one address (BEV-004).
6. Invariant: no e-mail from the app contains the text of a question or answer, an order file, or anything that lets a browser other than the requester's sign in; and no e-mail reaches the app.

Requirements

- **BEV-001 Baseline.** The app MUST meet the baseline of SEC-017, set only cookies with the `__Host-` prefix and refuse every request that changes something if it comes from another origin (LIVE-011).
- **BEV-002 Signing in as a customer.** A customer signs in with his e-mail address and a sign-in link. The link MUST sign in only in the browser that requested it; another browser, or a mailbox scanner, does not sign in with it and does not use it up. The e-mail also shows the link's code, to paste or copy into the browser of the request; the code field allows pasting and filling in by the browser (TOE-004). A link and its code are valid for 10 minutes, can be used once, and expire on a new request or after 5 wrong attempts. The app has no passwords.
- **BEV-003 No enumeration.** A sign-in request MUST get the same response, in about the same time, whether the e-mail address belongs to a customer, to a blocked customer or to no one. Only an address with access gets the e-mail (SCH-011).
- **BEV-004 Limits.** The app MUST refuse: more than 5 sign-in requests per hour per e-mail address, more than 20 sign-in requests per hour per IP address, more than 20 questions per day per customer, a question or answer of more than 2,000 characters (GEG-009), and more than 100 opened order files per day per customer.
- **BEV-005 Sessions.** A session on the Customer portal MUST end after 14 days without use, a session in Office after 12 hours without use. Signing out ends the session on the server. At every sign-in the session gets a new key.
- **BEV-006 Signing in as an employee.** An office employee and an administrator MUST sign in to Office with a passkey, which he registers on his invitation through Organisation management. Office sends no sign-in link, not even for recovery: it would let whoever reads along in a mailbox get around the passkey (G4). If an employee has no passkey on a device, then (a) a passkey that his own password manager syncs works, on each of his devices; (b) otherwise the administrator sends him a new invitation in Organisation management, confirmed with the administrator's passkey (ROL-010), and with it the employee registers a new passkey. There is one administrator and only he invites. The administrator MUST therefore register two passkeys, on two devices, at his first sign-in. If he still loses both, the Organisation asks for it in the platform (INV-001); after confirmation by the Decision maker there, Appwinst sends a new invitation for the administrator role.
- **BEV-007 Text stays text.** The text of a question and an answer MUST be stored and shown as plain text; an address in it does not become a clickable link. Every page MUST send a strict Content Security Policy and load no third-party script or inline script.

- **BEV-008 Attachments from Exact Online.** An attachment MUST open in the browser only if its content is PDF, JPEG or PNG, with the headers `Content-Security-Policy: sandbox` and `X-Content-Type-Options: nosniff`; every other attachment only as a download. The app does not pass on an attachment larger than 25 MB (KOP-005).
- **BEV-009 Secrets.** The client secret and the refresh token MUST be only in the secret store (SEC-006), the access token only in memory; none of the three is in the database, a log, an error message, an address or an e-mail. Logs contain only keys, no names, e-mail addresses or text of questions (SEC-016, VAST-006).
- **BEV-010 Outgoing requests.** The server MUST send requests only to Exact Online's host and to the service that sends the e-mail. An address Exact Online returns, he fetches only over HTTPS and on Exact Online's host. Every request has a timeout (KOP-008).
- **BEV-011 E-mail.** An e-mail from the app MUST contain only a short notice and a link (MEL-003), never the text of a question or answer, an order file or an attachment.
- **BEV-012 Tested separation.** Automated tests MUST call every address of the Customer portal with the keys of an order, order file and question of another relation, and fail the build if one returns data (as SEC-008 demands for Appwinst). A test MUST make every route of the integration fail on any request other than GET.
- **BEV-013 Breaches.** Appwinst reports a personal data breach to the installation company as SEC-015 says; the notification to the Dutch Data Protection Authority (AP) and to data subjects belongs to the installation company (VKL-004).
- **BEV-014 Destination after signing in.** If the app opens, after signing in, the page someone had to sign in for (SCH-012, SCH-042), that destination MUST be a path within the same portal. The app ignores any other destination; it then opens Orders or Questions.
- **BEV-015 No incoming e-mail.** The app MUST NOT receive e-mail: the sending domain has a null MX (RFC 7505; MEL-002), and the app has no address, mailbox or entry point that accepts e-mail.

If a part is in an attacker's hands

- **The production server.** The attacker reads the database (names and e-mail addresses, questions and answers, data of orders and order files) and, from the server's memory and secret store, the refresh token, and with it the administration within the scopes. He finds no attachments (KOP-005). So it does not cost everything: the installation company revokes the app in Exact Online or replaces the client secret, and the integration is closed; Appwinst treats it as Critical (BEH-003) and reports it (BEV-013).
- **A stolen backup.** Encrypted (SEC-007); it contains no tokens, because they are not in the database (BEV-009), and no attachments.

- **A customer's mailbox.** Whoever controls it signs in as that customer. The administrator blocks him (ROL-007).
- **An employee's mailbox.** Gives no access to Office: only a passkey signs in there (BEV-006).
- **Exact Online itself.** Falls outside this app; the subscription belongs to the installation company (VKL-005).

Residual risk

1. Whoever controls a customer's mailbox controls his access. Accepted: that is how every sign-in by e-mail works; the administrator blocks.
2. While VRAAG-KOP-1 is open, whoever fully controls the production server can write in Exact Online with the token, within the rights of the account that authorised the integration. Reduced by KOP-003 (an account with the smallest rights).
3. If a contact disappears from Exact Online, he keeps access until the next sync that sees it: at most 10 minutes, or until the nightly full read if VRAAG-KOP-3 is no. If someone must go at once, the administrator blocks.
4. The status in the app is at most 10 minutes behind Exact Online (KOP-004); the screen shows the time of the data (KOP-009).
5. If the administrator loses both passkeys, no one in the app invites an employee until Appwinst invites the administrator role again (BEV-006). Accepted: a quicker route would let someone get around the passkey.

12. Privacy

- **AVG-001 Roles.** The installation company is the controller (VKL-004). Appwinst is the processor under the data processing agreement, signed before Day 0 (PRIV-001; WK-001 item 6), with the sub-processors PRIV-002 names. Exact Online is a processor of the installation company itself: the app reads there on the installation company's instructions, and Exact Online is not a sub-processor of Appwinst.
- **AVG-002 No special data.** The app processes no special categories of personal data, no criminal data, no citizen service number (BSN) and no data of children: the Build request names none of these, and the customers are contacts of companies and schools, not pupils.
- **AVG-003 Every item with its purpose.** The app processes only the personal data below. How long they are kept is in Records and audit (VAST-007, and VAST-001 for a record), or here where those do not name the item.

Name and e-mail address, with the key of the contact and his relation in Exact Online. Of whom: customers. Purpose: signing in, showing the customer with his questions, sending him e-mail. Source: the integration. Kept: VAST-007.

Block: the normalised e-mail address and the relation, who blocked and when. Of whom: customers, employees. Purpose: refusing access

permanently, also when the address disappears from Exact Online and comes back (ROL-007), and saying who decided that. Source: the administrator. Kept: until the administrator restores access or the relation disappears (VAST-007).

Name, e-mail address and role of an employee. Of whom: employees. Purpose: signing in, showing the employee with his answers. Source: Organisation management. Kept: VAST-007.

Questions and answers, with who wrote them and when, when a customer opened an answer, and who closed a question. Of whom: customers and employees. Purpose: handling and finding again a question about an order. Source: what users enter. Kept: VAST-007.

Who changed the document types by kind, and when (only the administrator's identification, VAST-004). Of whom: the administrator. Purpose: saying who decided what customers see (ROL-006). Source: the administrator. Kept: VAST-001.

Sign-in link. Of whom: customers. Purpose: signing in. Source: the app. Kept: VAST-007.

Data of orders and order files, such as the subject of a document. Of whom: sometimes a name in a subject. Purpose: showing what belongs to an order. Source: the integration. Kept: as long as they are in Exact Online (GEG-011).

The content of work orders, invoices and documents, with the names and addresses in them. Of whom: whoever is in them. Purpose: showing with an order. Source: the integration. Kept: not: passed on, not kept (GEG-007, KOP-005).

IP address. Of whom: visitors. Purpose: limiting abuse (BEV-004). Source: the browser. Kept: only in memory, at most 1 hour.

Server and access logs. Of whom: everyone, with keys only. Purpose: finding faults and abuse. Source: the app. Kept: VAST-006.

Backups of all of the above. Of whom: everyone. Purpose: restoring. Source: the app. Kept: PRIV-007.

The app does not keep a contact without an e-mail address (GEG-002). The Counts of Core process (VAST-003) are not personal data: they name no person and no order. What someone writes back to an e-mail from the app does not reach the app (BEV-015). After the period the app MUST delete the item. If the installation company agrees a different period in the data processing agreement (PRIV-007, the row Client app production data), that is a new version of this document (ALG-005).

- **AVG-004 As little as possible.** The app reads only the fields of KOP-002, never a phone number (BUITEN-008), keeps no attachments from Exact Online (KOP-005), sets only the session cookie (BEV-001)

and uses no analytics or tracking cookies (MEET-002). Data about a person is corrected only in Exact Online, the source (VKL-002).

- **AVG-005 What customers see of each other.** The customers of one relation see, with an order of that relation, each other's questions, with the name of who asked, and the answers (ROL-004, VRG-003). A customer of another relation sees none of it.
- **AVG-006 Data subjects' rights.** A request for access, correction or deletion is answered by the installation company as controller; Appwinst helps free of charge with what it holds, and also with a data protection impact assessment if the installation company finds one necessary (PRIV-011). The installation company gets an export of all data through the platform at any time (BEH-011).
- **AVG-007 Privacy by design and security of processing.** AVG-004, ROL-001 and KOP-005 give effect to GDPR Article 25, the Security chapter to GDPR Article 32 ([27]). All data is in the EU (INV-009).

13. Accessibility and language

- **TOE-001** The app is in English (BUITEN-010). Every page and every e-mail carries English as its language. Texts from Exact Online, such as a description, the app shows as they are there.
- **TOE-002** Every screen MUST meet WCAG 2.2 level AA ([41]) and pass the automated accessibility gate (A11Y-006). This document makes no exception.
- **TOE-003** A status, an access and the label New answer MUST NOT rely on colour alone: each has text, and a status also its own icon.
- **TOE-004** Signing in asks for no password and nothing to remember. The sign-in link works without copying anything; the sign-in code is only a fallback, and its field allows pasting and lets the browser fill in the code; an employee signs in with a passkey. So signing in meets WCAG 2.2, success criterion 3.3.8 ([41]). The e-mail field lets the browser fill it in.
- **TOE-005** After sending a question or answer, after closing, after blocking and after restoring access, a screen reader MUST read out the confirmation without the focus moving (WCAG 2.2, success criterion 4.1.3, [41]).
- **TOE-006** Every link to an attachment names the kind and the subject of the order file and the file type. The accessibility of the attachments themselves is that of the attachments in Exact Online (VKL-002).
- **TOE-007** Every screen works with the keyboard alone, in an order the reader follows, with a visible focus. Every target to tap meets WCAG 2.2, success criterion 2.5.8. Every screen stays usable when zoomed to the limit of success criterion 1.4.10, without scrolling horizontally ([41]).
- **TOE-008** The app respects the setting for reduced motion.

- **TOE-009** The words are those of Terms: short and clear, without jargon. The statuses are named as in STAT-001.
- **TOE-010** The app is not offered to consumers. A draft accessibility statement is therefore not part of the Handover (A11Y-007).

14. Not-list

The public Not-list of Appwinst applies to this Build in full (the Appwinst specification, NIET-003). This Build adds the following items.

- **BUITEN-001 Read-only from Exact Online.** The app MUST NOT write anything in Exact Online. Orders, work orders, invoices, documents and contacts change only in Exact Online.
- **BUITEN-002 No import file.** The Build imports no file. The contacts and their relations come through the integration with Exact Online.
- **BUITEN-003 No maintenance scheduling.** In this Build a customer does not choose a time for maintenance. That is the Bookings add-on: option 2 of the Fit check, or later with Keep building.
- **BUITEN-004 No status history from before Live.** Exact Online keeps only an order's current status. The app records status changes from Live, not before.
- **BUITEN-005 No payments.** The app shows the invoice with an order. Paying happens outside the app.
- **BUITEN-006 No track and trace.** The app shows the status and the planned date of an order (STAT-001, STAT-002), not a carrier's route.
- **BUITEN-007 No attachments with a question.** A question is text. Customers and office employees add no attachments to a question or answer.
- **BUITEN-008 No phone numbers.** The app does not read or keep a contact's phone number.
- **BUITEN-009 E-mail as the only notification.** The app notifies by e-mail. There is no SMS, WhatsApp or push notification.
- **BUITEN-010 English only.** The app is in English. Another language is the Translation module add-on.
- **BUITEN-011 No app in an app store.** The app works in the browser on desktop, tablet and phone. An app in the App Store is the Native app, its own Extra sprint after Live.
- **BUITEN-012 No audit trail.** The app records what Records and audit names. An audit trail with export is the Audit trail add-on and is not in this Build.
- **BUITEN-013 No support to customers by Appwinst.** The installation company's office employees answer the customers' questions. Appwinst helps the installation company's organisation, through the platform.

15. Done when

The installation company answers each criterion with yes or no by using the app: in the Preview on test data, and after Live in the app itself (BB-003). Only these criteria decide whether a Pin is a Bug or a Wish (PIN-016). After each criterion is what it tests.

Customer portal: Sign in

- **KLAAR-001** A customer requests a sign-in link on Sign in with the e-mail address that is with his contact in Exact Online, and with the link from the e-mail is in Orders, without a password, in at most 2 steps on Mobile. (PROC-001, REIS-001, SCH-010, SCH-012.)
- **KLAAR-002** Whoever enters on Sign in an e-mail address without access, unknown or blocked at every relation, sees the same notice as for an address with access, and gets no e-mail. (SCH-011, BEV-003.)
- **KLAAR-003** A sign-in link that has already been used or is older than 10 minutes does not sign in; it opens a page that says so, with one button for a new link. (SCH-013, BEV-002.)
- **KLAAR-004** A sign-in link opened in a browser other than the browser that requested it does not sign in; with the sign-in code from the same e-mail, typed or pasted, the customer does sign in in the browser of his request. (SCH-011, SCH-012, BEV-002, TOE-004.)
- **KLAAR-043** The page a customer sees when he opens the sign-in link in another browser says that the link works only in the browser in which he requested it and that he can enter the sign-in code from the e-mail there; the page does not show the sign-in code. (SCH-014.)

Customer portal: Orders

- **KLAAR-005** Orders shows only the orders of the customer's relation, the current ones first, each with order number, description, status and, where STAT-002 says so, the planned date. (PROC-002, SCH-020, SCH-021, INVAR-001.)
- **KLAAR-006** From the e-mail with the sign-in link, a customer sees the status and the planned date of an order of his relation in at most 3 steps on Mobile. (PROC-002, REIS-002.)
- **KLAAR-007** Every order shows exactly one status, the one STAT-001 gives for its values in Exact Online, never empty and never beside a second status; the planned date is there only where STAT-002 says so. (STAT-001 to STAT-003, INVAR-004.)
- **KLAAR-008** If a customer's relation has no current order, Orders says so in the place of Current, with how the customer reaches the installation company, and the earlier orders are below it; no empty list. (SCH-024.)
- **KLAAR-009** A customer who is at two relations with the same e-mail address signs in once, chooses a relation in Orders and then sees only its orders; he can also choose the other relation. (SCH-023, GEG-003, ROL-005.)

Customer portal: Order

- **KLAAR-010** From Orders, a customer opens the attachment of a work order of an order in at most 2 steps. (PROC-003, REIS-003, SCH-031.)
- **KLAAR-011** Order always shows the three groups work orders, invoice and documents. Every order file that is with that order in Exact Online and whose document type has a kind according to Document types by kind is in its group, once, with subject and date, and each of its attachments opens. (PROC-003, SCH-030, SCH-031, GEG-005, GEG-006, KOP-005.)
- **KLAAR-012** A group without order files says in Order that there are no order files in it yet; an order without order files thus shows three empty groups and the field for a question. (SCH-031, SCH-033.)
- **KLAAR-013** An order file whose document type has no kind in Document types by kind, or is not in that table, the app shows to no one, not in Office either. (ROL-006, GEG-006.)
- **KLAAR-014** A customer who opens the address of an order, order file or question of another relation gets the same "not found" page as for an order that does not exist, and nothing of that order. (SCH-005, ROL-009, INVAR-001.)
- **KLAAR-015** A customer types a question in Order and sends it in 1 step; the question is then with that order, with the time, and the screen says that he gets an e-mail when there is an answer. (PROC-004, REIS-004, SCH-032, INVAR-006.)
- **KLAAR-016** Another customer of the same relation sees that question with the same order; a customer of another relation sees it nowhere. (VRG-003, AVG-005.)
- **KLAAR-017** With every question and every answer is who wrote it and when, and no one can change or delete a sent question or a sent answer. (VRG-001, VRG-004, GEG-009.)
- **KLAAR-018** A question of more than 2,000 characters is not sent; the app says how many characters are allowed, and the text stays. (GEG-009, BEV-004.)

Office: Sign in and Organisation management

- **KLAAR-019** An employee signs in to Office with his passkey; Office sends no sign-in link. A customer cannot sign in there, not even with his own e-mail address. (SCH-040, SCH-041, ROL-008, BEV-006.)
- **KLAAR-044** If an employee cancels signing in, or it fails, Office: Sign in says so, with a button to try again; if he has no passkey on this device, the screen says that he asks the administrator for a new invitation. (SCH-040, SCH-043.)
- **KLAAR-045** An employee whose passkey is synced by his password manager also signs in with that passkey on a second device. (BEV-006.)

- **KLAAR-020** An administrator invites a new office employee in Organisation management and confirms it with his passkey; the employee registers his passkey on the invitation and signs in to Office with it. An employee the administrator removes sees nothing more at his next click. (ROL-003, ROL-007, ROL-010, BEV-006.)
- **KLAAR-046** An employee without a passkey on his device gets a new invitation from the administrator, confirmed with the administrator's passkey, registers a new passkey with it and then signs in. (BEV-006, ROL-010.)
- **KLAAR-047** An administrator gets past his first sign-in only once he has registered two passkeys. (BEV-006.)

Office: Questions and Question

- **KLAAR-021** A question with an order without an open question sends every office employee an e-mail with a link to Question; a next question with that order, while there is an open question, sends none. (PROC-004 to PROC-005, MEL-006.)
- **KLAAR-022** Questions shows every open question, the oldest at the top, with relation, order number, the customer's name and since when it has been open; an answered or closed question is not among them. (SCH-050, VRG-002.)
- **KLAAR-023** From Questions, an office employee answers an open question in at most 2 steps. (PROC-005, REIS-005, SCH-060.)
- **KLAAR-024** Question shows the status, the planned date and the order files of the order beside the questions and answers. (SCH-061.)
- **KLAAR-025** On an answer, every customer with an open question with that order gets exactly one e-mail with the order number and a link. A customer who is not signed in reaches that order through the link after signing in, and sees the answer there. (PROC-005, REIS-005, MEL-005, SCH-012, INVAR-007.)
- **KLAAR-026** An office employee closes an open question; it is then no longer among the open questions, the customer sees closed with that question, and he gets no e-mail. (SCH-062, VRG-002, MEL-008.)
- **KLAAR-027** If a colleague answers while an office employee is typing, he sees that answer on sending, and his own text stays. (SCH-064.)

Office: Customers

- **KLAAR-028** Customers shows per relation the contacts from Exact Online, each with name, e-mail address and access, and finds a contact by name, relation or e-mail address. (SCH-070, SCH-071.)
- **KLAAR-029** From Customers, an administrator blocks a customer's access at a relation in at most 3 steps, the confirmation with his passkey included. At his next click in an open session that customer sees nothing more of that relation; if he has no other relation, he also gets no more sign-in links. (REIS-006, SCH-072, ROL-007, ROL-010, INVAR-003.)

- **KLAAR-030** An office employee sees no button to block in Customers; an administrator does, and confirms the block with his passkey. (ROL-004, ROL-010.)
- **KLAAR-031** An administrator restores a blocked customer's access with his passkey, and that customer can sign in again. (SCH-072, ROL-010.)
- **KLAAR-032** A block of a customer at a relation stays in force after a sync, also if his e-mail address disappears from Exact Online and later comes back; it ends only when the administrator restores access or the relation disappears. Customers shows with Blocked who blocked and when. (GEG-010, ROL-007, SCH-070, SCH-073, VAST-001.)

The integration with Exact Online

- **KLAAR-033** A contact with an e-mail address whom the installation company adds in Exact Online to a relation with an order can sign in after the next sync and sees the orders of that relation, without anyone creating an account in the app or supplying a file. (GEG-002, GEG-003, IMP-004.)
- **KLAAR-034** A contact deleted from the test administration in Exact Online can no longer sign in after the nightly full read at the latest, not even in a session that was open; his questions are still with their order, with deleted contact as sender. (ROL-007, KOP-004, GEG-011, VAST-004.)
- **KLAAR-035** If the status of an order changes in the test administration, or an order or order file is added, that is in the app within 10 minutes, and the status change is in Question with that order, with the date on which the app saw it. (KOP-004, GEG-008, VAST-002, SCH-061, INVAR-005.)
- **KLAAR-036** If Exact Online cannot be reached, or the integration is broken, for example because the installation company has revoked the app in Exact Online, then Orders, Order and Customers show the last known data with the time at which they were updated, say that they are not current, and show no empty list. The administrator then gets one e-mail, and one more when the integration works again; none in between. (SCH-004, KOP-009, MEL-009, INVAR-005.)
- **KLAAR-037** After a week of using the Preview, no order, order file, contact or relation in the test administration has been changed by the app. (KOP-001, BUITEN-001, INVAR-002.)

E-mail and data

- **KLAAR-038** Whoever replies to an e-mail from the app gets his reply back as undeliverable; it does not become a question or answer, and the app does not receive it. Every e-mail from the app ends with its link. (MEL-002, MEL-003, MEL-007, BEV-015.)
- **KLAAR-039** No e-mail from the app contains the text of a question or answer, or an order file or other attachment. (MEL-003, BEV-011.)
- **KLAAR-040** Nowhere in the app, and not in the export of BEH-011, is there a contact's phone number. (GEG-002, KOP-002, BUITEN-008.)

The whole app

- **KLAAR-041** Every screen of both apps works on Mobile, Tablet and Desktop of the Preview and with the keyboard alone, and every status, access and every label can also be read without colour. (SCH-002, TOE-003, TOE-007, A11Y-006.)
- **KLAAR-042** The app counts every event that Core process names per day, without person, relation or order, and the counts are in the export of the data (BEH-011). (MEET-001, MEET-002, VAST-003; each journey its measure.)

16. Ownership, control and exit

- **EIG-001 The installation company keeps control.** INV-013 applies to this app. This chapter names what that means here and does not repeat the rules.
- **EIG-002 Code and rights.** The app's repositories follow INV-007 and LIVE-010; the copyright follows the IP deed (LEG-017); Fundamental comes with the licence of LIC-001 and its own Fundamental copy (MIR-002).
- **EIG-003 Domains.** The domain `voorbeeld.example` is in the installation company's name. The Customer portal is at `portal.voorbeeld.example` and Office at `office.voorbeeld.example`, connected as LIVE-011 says, beside their address at Appwinst. The DNS records of the sending domain (MEL-002), with its null MX (BEV-015), are in the installation company's domain.
- **EIG-004 Third-party accounts.** The Exact Online subscription, the app's registrations in the Exact App Center for test and production, and the developer subscription for the test administration (KOP-010) are in the installation company's name (VKL-005, INV-013). The installation company revokes the app in Exact Online whenever it wants; the integration then stops (KOP-009).
- **EIG-005 Data.** The installation company gets a full export through the platform at any time (BEH-011). Orders, work orders, invoices, documents and contacts stay in Exact Online; the app is never their source.
- **EIG-006 Maintenance.** Appwinst runs and maintains the app under Maintenance (BEH-001), on the basis of Maintenance Normal (BEH-008). The integration adds no server, no attachment storage and no service: the app reads on a schedule, keeps no attachments (KOP-005) and has no webhook (KOP-004). So there is no surcharge (BEH-009).
- **EIG-007 Exit.** On exit, the handover of BEH-012 applies and, without a choice after Live, LIVE-009. Appwinst then deletes the integration's credentials from its secret store (BEH-012); the installation company

SHOULD then replace the client secret in the Exact App Center or revoke the app there.

17. The client's responsibility

What the Appwinst specification places with the client in LEG-019 applies to this app as follows. The client here is the installation company; a customer in this document is always the customer role.

- **VKL-001 Operations and users.** The installation company alone is responsible for its operations, for the content and use of the app, and for its users: the customers and its own employees. What the installation company promises its relations, such as how quickly a question gets an answer, is its promise (LEG-019).
- **VKL-002 The data in Exact Online.** The installation company is responsible for the accuracy of the orders, work orders, invoices and documents in Exact Online. The app shows what Exact Online supplies.
- **VKL-003 Who has access.** A contact with an e-mail address at a relation that has a sales order in Exact Online can sign in as a customer and sees the orders of that relation. The installation company keeps the contacts in Exact Online accurate, and blocks whoever may no longer have access.
- **VKL-004 Controller.** The installation company is the controller of the personal data in the app: names and e-mail addresses, questions and answers, and the order files from Exact Online. Appwinst is the processor under the data processing agreement (PRIV-001; GDPR Article 28(3) [27]). The lawful basis for the processing is the installation company's (LEG-019).
- **VKL-005 Subscriptions and accounts.** The Exact Online subscription, the registration of the app in the App Center by the installation company's main user, and the Exact Online developer subscription with the test administration for the Preview (KOP-010) belong to the installation company, in its name and at its expense (INV-013, LEG-019). The app shares Exact Online's API limits per administration with the installation company's other apps [11]. The domain of both apps is in the installation company's name (LIVE-011).
- **VKL-006 The completion file.** On notice that the work is ready for completion, a contractor must give the client a file (Article 7:757a of the Dutch Civil Code [17], [18], [19]). That duty stays with the installation company. The app shows documents with an order; whether and how the installation company delivers the file with them, the installation company decides.
- **VKL-007 Liability.** The installation company indemnifies Appwinst as LEG-019 says. Appwinst's liability for its own performance is that of LEG-015; this document adds nothing to it and takes nothing from it.

18. Conformance

- **CONFORM-001** The app conforms to this specification when every criterion of Done when is answered with yes and no requirement of this document is broken. Before Live every criterion has its evidence (LIVE-001 item 1).
- **CONFORM-002** Every requirement is tested as follows:

Section	How it is tested
Invariants	An automated test per invariant, with two relations in the test data; for INVAR-001 and INVAR-003 the tests of BEV-012, and a test of a session after a block.
Roles and permissions	A test per role and per action of ROL-004, showing that everything the role is not expressly allowed is refused (ROL-001).
Domain model; Records and audit	Tests on the schema, on the read paths of GEG-013, and on what is recorded at every action.
Core process	The Demo runs PROC-001 to PROC-005 on test data (DEM-001); a test per event of MEET-001.
Screens	The criteria of Done when per screen, in the Preview, on Mobile, Tablet and Desktop.
Integration and import	The checks of KOP-010 and BOUW-002 before the Start; tests on recorded responses of the test administration; a test that makes every route of the integration fail on any request other than GET (BEV-012); KLAAR-033 to KLAAR-037 in the Preview.
Notifications	The e-mails in the Preview, where the app catches them (PRV-010); before Live the records of the sending domain (MEL-002), and that this domain accepts no mail (KLAAR-038).
Security	OWASP ASVS 5.0, level 2 [42], for both apps; the gates of §22 of the Appwinst specification; the tests of BEV-012.

Privacy	A check that the app keeps only the data of AVG-003, and no phone number (KLAAR-040).
Accessibility and language	The automated accessibility gate (A11Y-006) on every screen, and KLAAR-041 with keyboard and screen reader, against WCAG 2.2 level AA [41].

- **CONFORM-003** The Customer portal SHOULD meet, on Sign in, Orders and Order on Mobile, the "good" thresholds of Core Web Vitals that the Appwinst specification sets in §23 for its own sites: LCP at most 2.5 s, INP at most 200 ms and CLS at most 0.1, at the 75th percentile; and the server SHOULD respond on those screens within 500 ms at the 95th percentile. Opening an attachment does not count: the app fetches it from Exact Online (KOP-005), and how fast that goes depends on Exact Online.
- **CONFORM-004** Office SHOULD meet, on Sign in, Questions, Question and Customers on Desktop, the same thresholds as CONFORM-003.
- **CONFORM-005** CONFORM-003 and CONFORM-004 are measured on the Test version, with test data, on the profile Mobile or Desktop; after Live the monitoring of Maintenance measures the server's response time (BEH-001).
- **CONFORM-006** Under Maintenance, for each of the two portals the availability of BEH-005 and the recovery of BEH-013 apply, in the form of Maintenance the installation company chooses (BEH-001).

19. Build plan by day

The build plan follows the build week of the Appwinst specification (§7). The Build brief gives each day with its date and times (CAL-011). The foundation is in place before the Start (CAL-013). After that each section builds its own code paths, at most a build day of work, with its own developer, so that the sections are built side by side (BC-016).

- **BOUW-001** The foundation MUST be finished before the Start: the data model (Domain model); signing in to both apps as Security says, with the sign-in link and sign-in code for customers and the passkey for employees, with the roles and everything refused by default (ROL-001); the integration with Exact Online (KOP-001 to KOP-009), with the sync and its state; the derivation of the status (STAT-001); the access check on every request (INVAR-001, INVAR-003); sending e-mail through the outbox (GEG-012), from the address of MEL-002; counting the events (MEET-001); both apps in the brand of the brandbook, with the place in Order where the questions go; and the test users, one per role (PRV-008).

- **BOUW-002** The test administration is in the installation company's developer subscription (KOP-010). Besides the checks of KOP-010, the Builder MUST record in it before the Start that it contains: at least two relations with an order, each with at least one contact with an e-mail address; for each of the five statuses of STAT-001 an order, and in addition an open order with a planned date that has passed; a relation with only earlier orders; an order without order files; and a relation without a sales order, with a contact with an e-mail address, who cannot sign in (VKL-003). He checks that the field the installation company named before signing as its answer to VRAAG-ROL-1 is filled on every order (ROL-005). With the installation company he settles in the test administration: the document types by kind (GEG-006); a contact's e-mail field (IMP-003); the fields for an order's description, and for the subject and date of an order file and the file name, file type and size of its attachments (SCH-021, SCH-030, SCH-031); and how many orders a relation has and how many order files an order (GEG-014). If anything is missing, item 4 of WK-001 is not done and the Builder says what is missing (WK-002).
- **BOUW-003** The sections are:

Section	What	Criteria
A	Customer portal: Orders and Order, with the order files, the choice of relation, the empty states and the state of the integration	KLAAR-005 to KLAAR-014
B	Office: Customers, with blocking and restoring access; inviting employees with Organisation management, with their passkey; the document types by kind and the state of the integration in the Management area	KLAAR-020, KLAAR-028 to KLAAR-032, KLAAR-046, KLAAR-047
C	Customer portal: the question in Order and the answers below it (A5)	KLAAR-015 to KLAAR-018
D	Office: Questions and Question, with closing, and the e-mails on a new	KLAAR-021 to KLAAR-027, KLAAR-039

	question and a new answer (A5)

The foundation covers KLAAR-001 to KLAAR-004, KLAAR-019, KLAAR-033 to KLAAR-038, KLAAR-040 and KLAAR-042 to KLAAR-045; each section covers KLAAR-041 for its own screens.

Day	What happens
Before Day 0	The foundation (BOUW-001), built on Exact Online's documented API.
Day 0	The checks of KOP-010 and BOUW-002, in the test administration of the installation company's developer subscription. The Build becomes Ready to start when every item of WK-001 is done.
Day 1	Start. Sections A, B, C and D are built side by side. The Preview is live with signing in, Orders and Order on the test administration (PRV-001).
Day 2	The sections are finished. The Demo runs PROC-001 to PROC-005 (DEM-001).
Day 3	The stop button window closes (DEM-008). Wishes from Pins up to the feedback limit of §7; the production environment in the EU is set up.
Day 4	The Test version: after that only Bugs (WK-012). Production runs, with backups and a tested restore (LIVE-001 item 4). The installation company gives access to its production administration through the secrets form (KOP-011, LIVE-001 item 6).
Day 5 and 6	No building (WK-013). Pins can be placed in the Preview.
Day 7	Live. The app syncs with the production administration; no customer gets an e-mail of its own accord. The administrator registers his passkeys at his first sign-in

	(KLAAR-047). The portals run at their address at Appwinst, and at the installation company's own addresses once its DNS has the record of LIVE-011 (EIG-003). The Handover for Live (LIVE-003).

20. Appendix: configuration values

Every setting of the app, with the requirement that sets it (ALG-005). A value settled on Day 0 is, after BOUW-002, in the report of Day 0 and counts as part of this Appendix.

The integration with Exact Online

Value	Setting	Requirement
Sync of changes	every 5 minutes	KOP-004
Full read of contacts and relations	every night	KOP-004
Own daily budget of calls	4,000 calls per day, of which 1,500 calls per day free for the sync	KOP-007
Error limit per endpoint	3 failed calls per hour	KOP-008
Timeout of a call	30 seconds	KOP-008
Largest attachment the app passes on	25 MB	KOP-005, BEV-008
The field of a sales order that binds it to its relation	the field the installation company names before signing (VRAAG-ROL-1); on Day 0 the Builder checks that it is filled	ROL-005, BOUW-002
A contact's e-mail field	`Email` or `BusinessEmail`, settled on Day 0	IMP-003
The fields for an order's description, and for the subject, date, file name, file type and size of an order file and its attachments	settled on Day 0	BOUW-002

Data the administrator manages (not a setting, ALG-005)

Value	Initial state	Requirement
Document types by kind (work order, invoice, document or not visible)	settled on Day 0; after that the administrator	GEG-006, ROL-006

	changes them in the Management area	

Signing in, sessions and limits

Value	Setting	Requirement
Validity of a sign-in link and its sign-in code	10 minutes	BEV-002
Wrong attempts per sign-in link	5 wrong attempts	BEV-002
Session on the Customer portal	14 days without use	BEV-005
Session in Office	12 hours without use	BEV-005
Fresh confirmation with the passkey	within the last 10 minutes	ROL-010
The administrator's passkeys at his first sign-in	two	BEV-006
Sign-in requests	at most 5 sign-in requests per hour per e-mail address, and 20 sign-in requests per hour per IP address	BEV-004
Questions per customer	at most 20 questions per day	BEV-004
Opened order files per customer	at most 100 opened order files per day	BEV-004
Longest question or answer	2,000 characters	GEG-009, BEV-004

Keeping

Value	Setting	Requirement
The conversation with an order, with its closings	24 months after the last message or the last closing in the conversation, or shorter if the order disappears from Exact Online	VAST-007
A contact's name and e-mail address	as long as they are in Exact Online; deleted at the sync that sees they are no longer there	VAST-007, GEG-011

A block	until the administrator restores access, or until the relation disappears from the app	VAST-007, GEG-010
An employee's name, e-mail address and role	until the administrator removes him in Organisation management	VAST-007
Counts of Core process	13 months	VAST-001
IP address	only in memory, at most 1 hour	AVG-003

E-mail and texts

Value	Setting	Requirement
Sending domain	`mail.voorbeeld.example`, a domain that accepts no mail	MEL-002
How a customer reaches the installation company, when there are no current orders	a text in Texts and images	SCH-024

Speed

Value	Setting	Requirement
LCP on the main screens, 75th percentile	2.5 s	CONFORM-003, CONFORM-004
INP on the main screens, 75th percentile	200 ms	CONFORM-003, CONFORM-004
CLS on the main screens, 75th percentile	0.1	CONFORM-003, CONFORM-004
Server response time on the main screens, 95th percentile	500 ms	CONFORM-003, CONFORM-004