



Integrated Control Technology Ltd

Data Management Overview

Last Published: 17-Nov-25



Contents

Introduction	3
ICT Products	4
Protege WX	4
Protege X	5
Protege GX	6
Mobile Credential Portal	7
Protege Tenancy Portal	8
Protege Mobile App	9
Protege Config App	10
Offline Wireless Locks	10
ICT Websites	11
ICT Marketing Website	11
ICT Partner Website	12
Third-Party Platforms	13
Docebo Learning Management System (LMS)	13
Online Ordering	14
Salesforce	15
Marketing Cloud Account Engagement (MCAE)	16
Google Analytics	17
Zendesk for Customer Service	18
Zendesk for Technical Support	19
SAP S/4HANA	20

Introduction

This document covers the types of personal data collected by ICT products, websites and services, and how this data is stored and handled.

For more information about how ICT handles your personal data, see our Privacy Policy at <https://ict.co/privacy-policy/>.

Please note that if a user is habitually resident in the United Kingdom (UK) or European Economic Area (EEA), they may benefit from additional rights and protections under the UK or EU General Data Protection Regulation (GDPR). This document outlines how ICT manages personal data globally, but some provisions—including access to individual rights—apply only to those residing in these jurisdictions.

ICT Products

Protege WX

- **Purpose:** User account data is stored to manage site access, determine system access for monitoring and configuration and store an audit trail tracking user and system activities.
- **Data:** User account details (e.g. first name, last name), card and PIN numbers, usernames and passwords, login timestamps, system activity logs, and configuration settings.
- **Method:** Accounts are created and managed by system admins. Activity logs are collected upon login and system interactions.
- **Storage:** Data is stored on the Protege WX device (controller) only.
- **Third-party:** Some integrations with other products — for example, but not limited to, video management systems, elevator control, biometric readers — require user data to be shared to enable their functionality. The data is not shared with these third-party products without informed consent from the data subject or reliance on another valid legal basis (where applicable for data subjects usually resident in the UK or EEA). All integrations provided by ICT are installed and configured by ICT dealers.
- **EUSCC:** Logins are protected by a username and password.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.

In cases where ICT is the data processor, ICT uses commercially reasonable efforts to ensure that the data controller has implemented a valid lawful basis for data collection (for example via contractual terms with data controller) and only where applicable for data subjects usually resident in the EEA or UK, save that the overall responsibility for compliance remains with the data controller.

- **Retention:** User account data is retained only for as long as necessary for the purposes for which it is processed, or as required by applicable law. User data may remain in the system for as long as the account remains active and the database has sufficient space to store it. System logs follow the same principles. Users are not able to self-delete, but can request that an administrator delete their data.

User data may be retained in system backups for a certain period of time, depending on the system owner’s policies.

Protege X

- **Purpose:** User account data is stored to manage site access, determine system access for monitoring and configuration and store an audit trail tracking user and system activities.
- **Data:** User account details (e.g. first name, last name), card and PIN numbers, usernames and passwords, login timestamps, system activity logs, and configuration settings.
- **Method:** Accounts are created and managed by system admins. Activity logs are collected upon login and system interactions.
- **Storage:** Data is stored in a cloud hosted database (Microsoft Azure) and on the Protege WX device (controller).
- **Hosting Region:** USA.
- **Third-party:** Some integrations with other products — for example, but not limited to, video management systems, elevator control, biometric readers — require user data to be shared to enable their functionality. All integrations provided by ICT are installed and configured by ICT dealers.
- **EUSCC:** N/A—service is not available in EU or UK regions.
- **Lawful Basis:** N/A—service is not available in EU or UK regions.
- **Retention:** User account data is retained only for as long as necessary for the purposes for which it is processed, or as required by applicable law. User data may remain in the system for as long as the account remains active and the database has sufficient space to store it. System logs follow the same principles. Users are not able to self-delete, but can request that an administrator delete their data.
User data may be retained in system backups for a certain period of time, depending on the system owner's policies.

Protege GX

- **Purpose:** User account data is stored to manage site access, determine system access for monitoring and configuration and store an audit trail tracking user and system activities.
- **Data:** User account details (e.g. first name, last name), card and PIN numbers, ID photos, biometrics (e.g. fingerprint, face scan), email address, usernames and passwords, login timestamps, system activity logs, and configuration settings.
- **Method:** Accounts are created and managed by system admins. Activity logs are collected upon login and system interactions.
- **Storage:** Data is stored within the Protege GX database, primarily on-premises. Some system owners deploy to cloud-hosted environments. Data is also stored on the Protege GX device (controller).
- **Third-party:** Some integrations with other products — for example, but not limited to, video management systems, elevator control, biometric readers — require user data to be shared to enable their functionality. The data is not shared with these third-party products without informed consent from the data subject or reliance on another valid legal basis (where applicable for data subjects usually resident in the UK or EEA). All integrations provided by ICT are installed and configured by ICT dealers.
- **EUSCC:** Logins are protected by a username and password.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.

In cases where ICT is the data processor, ICT uses commercially reasonable efforts to ensure that the data controller has implemented a valid lawful basis for data collection (for example via contractual terms with data controller) and only where applicable for data subjects usually resident in the EEA or UK, save that the overall responsibility for compliance remains with the data controller.

- **Retention:** User account data is retained only for as long as necessary for the purposes for which it is processed, or as required by applicable law. User data may remain in the system for as long as the account remains active and the database has sufficient space to store it. Users are not able to self-delete, but can request that an administrator delete their data.

User data may be retained in system backups for a certain period of time, depending on the system owner’s policies.

Mobile Credential Portal

- **Purpose:** Mobile credentials solution stores user data to send emails on availability of credentials and to provide accounts to use those credentials.
- **Data:** Email, device serial number, make and model, user account preferences, last used date/time. May also store connection data for Protege GX, Protege WX or Protege X site.
Credential value is generated by ICT and used by Protege GX, Protege WX or Protege X to provide access.
- **Method:** Accounts are created in the credential portal by building administrators. ICT emails to inform the user that a credential is available. The user creates an app account to access their credential.
- **Storage:** Hosted by Microsoft Azure.
- **Hosting region:** USA. Personal data transferred from the EEA and UK to the USA is conducted under the EU-U.S. Data Privacy Framework certification and UK Extension where applicable. For transfers not covered by this framework, Standard Contractual Clauses (SCCs), the UK Addendum, and supplementary measures are implemented in accordance with GDPR and UK GDPR requirements, as applicable.
- **Third-party:** Credential portal is hosted by Microsoft Azure.
- **EUSCC:** Credential portal logins are protected by username/password. It is possible to self-register an account, but no services will be available without invitation from an administrator. No end-user access. SSL protected site.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.
In cases where ICT is the data processor, ICT uses commercially reasonable efforts to ensure that the data controller has implemented a valid lawful basis for data collection (for example via contractual terms with data controller) and only where applicable for data subjects usually resident in the EEA or UK, save that the overall responsibility for compliance remains with the data controller.
- **Retention:** Users can self-delete their app accounts. Building administrators can delete user data from the credential portal.

Protege Tenancy Portal

- **Purpose:** Tenancy portal stores user email addresses or phone numbers to link to a mobile app account. Data is synced to an entry station device to allow SIP calls.
- **Data:** Requires tenancy name (e.g. apartment number) and email address or phone number. The tenancy portal generates a unique SIP extension for each user, which is used on the PBX server to place the call.
- **Method:** Accounts are created in the tenancy portal by building administrators. Alternatively, the building admin may sync account data from Protege GX to the tenancy portal. Name and tenancy are added to a phone book and displayed on a device at building entrance.
- **Storage:** Data is stored on the tenancy portal, hosted by Microsoft Azure. SIP extensions are stored on the PBX server. Data is downloaded to one or more entry stations on-premises.
- **Hosting region:** USA. Personal data transferred from the EEA and UK to the USA is conducted under the EU-U.S. Data Privacy Framework certification and UK Extension where applicable. For transfers not covered by this framework, Standard Contractual Clauses (SCCs), the UK Addendum, and supplementary measures are implemented in accordance with GDPR and UK GDPR requirements, as applicable.
- **Third-party:** The tenancy portal is hosted by Microsoft Azure.
- **EUSCC:** Logins are protected by username/password. No user registration flow - must be a known existing user to access. No end-user access. SSL protected site.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.

In cases where ICT is the data processor, ICT uses commercially reasonable efforts to ensure that the data controller has implemented a valid lawful basis for data collection (for example via contractual terms with data controller) and only where applicable for data subjects usually resident in the EEA or UK, save that the overall responsibility for compliance remains with the data controller.
- **Retention:** Users can self-service delete their mobile app accounts, preventing further SIP calls. If the user was added to the tenancy portal manually, a system administrator can remove the data. If the user data was synced from Protege GX, the administrator can remove the user from the synchronization to automatically delete their data from the tenancy portal.

Protege Mobile App

- **Purpose:** The Protege Mobile App is used to access mobile credentials provided by the credential portal, manage a physical site and receive SIP calls via the tenancy portal.
- **Data:** Email address, password, PIN, credentials, device serial number, make and model, user account preferences, last used date/time. May also store information for connecting to a Protege GX, Protege WX or Protege X site and/or information for connecting to a SIP server.
Data used for offline wireless locks is stored on the phone, including: access rights, access logs, blocklists.
- **Method:** Accounts are created in the credential portal by building administrators. ICT emails to inform the user that a credential is available. The user creates an app account to access their credential. Users must accept the terms and conditions and privacy policy to use the app.
Wireless lock data is transferred between wired card readers and wireless locks on-premises.
- **Storage:** Authentication keys are stored in the device's Secure Access Module (SAM).
Credential, user information and connection data for Protege GX, Protege WX or Protege X are stored in the credential portal (see page 7). SIP information is stored in the tenancy portal (see previous page).
- **Hosting region:** USA. Personal data transferred from the EEA and UK to the USA is conducted under the EU-U.S. Data Privacy Framework certification and UK Extension where applicable. For transfers not covered by this framework, Standard Contractual Clauses (SCCs), the UK Addendum, and supplementary measures are implemented in accordance with GDPR and UK GDPR requirements, as applicable.
- **Third-party:** Credential and tenancy portals are hosted by Microsoft Azure.
- **EUSCC:** Logins are protected by username/password.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.
In cases where ICT is the data processor, ICT uses commercially reasonable efforts to ensure that the data controller has implemented a valid lawful basis for data collection (for example via contractual terms with data controller) and only where applicable for data subjects usually resident in the EEA or UK, save that the overall responsibility for compliance remains with the data controller.
- **Retention:** Users can self-delete their app accounts. Building administrators can delete user data from the credential portal.

Protege Config App

- **Purpose:** The Protege Config App is used to access mobile credentials provided by the credential portal and configure ICT card readers and wireless locks.
- **Data:** Email address, password, PIN, credentials.
Data used for offline wireless locks is stored on the phone, including: access rights, access logs, blocklists.
- **Method:** Accounts are created in the credential portal by building administrators. ICT emails to inform the user that a credential is available. The user creates an app account to access their credential. Users must accept the terms and conditions and privacy policy to use the app.
Wireless lock data is transferred between wired card readers and wireless locks on-premises.
- **Storage:** Authentication keys are stored in the device's Secure Access Module (SAM).
Credential and user information are stored in the credential portal (see page 7). SIP information is stored in the tenancy portal (see page 8).
- **Hosting region:** USA. Personal data transferred from the EEA and UK to the USA is conducted under the EU-U.S. Data Privacy Framework certification and UK Extension where applicable. For transfers not covered by this framework, Standard Contractual Clauses (SCCs), the UK Addendum, and supplementary measures are implemented in accordance with GDPR and UK GDPR requirements, as applicable.
- **Third-party:** Credential and tenancy portals are hosted by Microsoft Azure.
- **EUSCC:** Logins are protected by username/password.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.
In cases where ICT is the data processor, ICT uses commercially reasonable efforts to ensure that the data controller has implemented a valid lawful basis for data collection (for example via contractual terms with data controller) and only where applicable for data subjects usually resident in the EEA or UK, save that the overall responsibility for compliance remains with the data controller.
- **Retention:** Users can self-delete their app accounts. Building administrators can delete user data from the credential portal.

Offline Wireless Locks

- **Purpose:** Hardware that grants or denies access based on the credential a user presents at the lock.
- **Data:** User data is not utilized during communication with the locks. The credentials carry a specific ID that is tied to the user in the system. The locks themselves only use and store these IDs.
- **Method:** The locks receive credential data and blocklists from user credentials and the configuration app. They save audit trails of credentials used, which are then stored on user credentials to be returned to the system.
- **Storage:** Data is stored in the locks and on user credentials. All data is encrypted.
- **Third-party:** N/A
- **EUSCC:** N/A (locks only available in North America)
- **Retention:** Each lock’s cache is updated on a rolling basis or until the data expires.

ICT Websites

ICT Marketing Website

- **Purpose:** Provides information on the company and its products and solutions.
- **Data:** Optional forms can collect user data including email address, name, company name, phone number, region (country, state), job title, user type, and query. The user's IP address may be captured when they visit certain web pages containing MCAE tracking codes (see page 16).
- **Method:** The user inputs data directly into website forms.
- **Storage:** No personal data is stored on the website.
- **Hosting Region:** N/A
- **Third Parties:**
 - Form data entered into website forms is sent to MCAE to create and update prospect records (see page 16). Cookies are also used to track engagement with marketing assets and sent to MCAE.
 - Basic pageviews and session data such as device types, operating system and browser type are sent to Google Analytics to analyze site performance (see page 17).
- **Retention:** No data is stored on retained on the website.
- **Lawful Basis:** N/A
- **Cookies:** Refer to <https://ict.co/privacy-policy/cookie-policy>

ICT Partner Website

- **Purpose:** Providing approved customers with access to software, firmware, and other gated resources that require a user to login. Users also use this portal to connect to the Docebo learning management system (LMS) and Zendesk ticketing system.
- **Data:**
 - **User records:** Name, email address, password (encrypted), country, phone numbers (optional), language preference (optional), company name, access permissions. Database also holds historical certification details (prior to LMS implementation) and support tickets (prior to Zendesk implementation).
 - **Company records:** Company name, address, phone numbers, website URL (optional), company type and distributor.
- **Method:** User data is synced from Salesforce when contact and account records are created or updated. Administrative users may also add users and companies directly through the site.
- **Storage:** Rimu Hosting.
- **Hosting Region:** New Zealand. ICT relies on the adequacy decision and regulation issued by the European Commission and UK Government for transfers from the EEA and UK to this region.
- **Third Parties:** Data is synced to linked records in Salesforce, Docebo LMS, and Zendesk.
- **Retention:** Personal data is retained only for as long as necessary for the purposes for which it was collected, in accordance with our data retention policy and applicable data protection laws. Users may request deletion of their personal data in accordance with their rights under applicable data protection legislation.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.

Some examples of ICT’s legitimate interests include maintaining the security of ICT’s system, conducting data analytics, responding to your communications, managing ICT’s business relationship with you, enhancing, modifying or improving ICT’s services and identifying usage trends. Where required by law and where such personal data is collected via cookies or other similar technologies, ICT otherwise only processes personal data for marketing purposes or analytics on the basis of user **consent**. Note that where consent is relied upon, ICT will not combine this lawful basis with any other, as we recognize this would be inherently unfair to user rights.
- **Cookies:** Refer to <https://ict.co/privacy-policy/cookie-policy>

Third-Party Platforms

Docebo Learning Management System (LMS)

- **Purpose:** User data is used to provide platform access, log learning activities, issue email notifications and allow segmentation for reporting purposes.
- **Data:** Includes name, email, company, and related details such as country and region, login timestamps, platform activity logs, certification and expiry details, learning activity and achievements.
- **Method:** All user data, other than learning activities performed within the platform, is synchronized from Salesforce, which is synchronized with the user's MyICT account. No adding or editing of user or company data occurs within the platform itself.
- **Storage:** Docebo's cloud servers.
- **Hosting Region:** Asia Pacific (Sydney, Australia) .Where personal data is hosted in Australia, which is not currently recognised by the European Commission or UK Government as providing an adequate level of protection, we implement Standard Contractual Clauses (SCCs) and, where applicable, the UK Addendum, along with supplementary technical and organizational measures in line with EU and UK GDPR requirements .
- **Third Parties:** Docebo is a third-party product. Users access the platform from their MyICT account using single sign-on. Docebo uses a secondary third-party product (Workato) to provide the synchronization from Salesforce, and uses Snowflake as a data warehouse and AWS QuickSight for the front-end analytics solution embedded into the platform.
- **Retention:** Personal data is retained only for as long as necessary for the purposes for which it was collected, in accordance with our data retention policy and applicable data protection laws. Users may request deletion of their personal data in accordance with their rights under applicable data protection legislation.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user's fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user's interests or fundamental rights and freedoms. ICT's legitimate interests relate to ICT's commercial interests and ICT's need to operate business to provide the requested goods and services.

Some examples of ICT's legitimate interests include maintaining the security of ICT's system, conducting data analytics, responding to your communications, managing ICT's business relationship with you, enhancing, modifying or improving ICT's services and identifying usage trends. Where required by law and where such personal data is collected via cookies or other similar technologies, ICT otherwise only processes personal data for marketing purposes or analytics on the basis of user **consent**. Note that where consent is relied upon, ICT will not combine this lawful basis with any other, as we recognize this would be inherently unfair to user rights.
- **Cookies:** No changes have been made to default Docebo settings: <https://help.docebo.com/hc/en-us/articles/360020125019-Cookie-Policy-Questions-answers>

Online Ordering

- **Purpose:** Customer data is collected and stored to generate sales orders, calculate unique product discounts, dispatch shipments to customer addresses and communicate order updates to customer email addresses.
- **Data:** Names, email addresses, addresses, phone numbers, product details unique to specific customers, software serial numbers, credential profile identifiers, site names and purchase order numbers.
- **Method:** User data is synchronized with Salesforce and SAP. Order-specific data is submitted by the customer and stored within Shopify and SparkLayer. Data is manually processed and uploaded to SAP for order dispatch.
- **Storage:** Shopify and Sparklayer cloud servers.
- **Hosting Region:** Shopify primarily uses Google Cloud Platform (GCP) for its server infrastructure, with data centers located in various regions including North America, Europe, Asia-Pacific, and South America. Where personal data is transferred outside the UK or EEA, ICT ensures that appropriate safeguards are in place under UK and EU data protection laws. These safeguards include the use of European Commission-approved Standard Contractual Clauses (SCCs), the UK's International Data Transfer Agreement (IDTA), or transfers to countries with adequacy decisions where the recipient is outside of the USA and is not certified under the EU-US data privacy framework and UK Extension.
- **Third Parties:** Shopify and Sparklayer are each third-party platforms with their own standards for data privacy and protection. Each platform meets acceptable best practices for data security.
- **Retention:** User data retention aligns with retention policies established by Shopify and Sparklayer.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.

Some examples of ICT’s legitimate interests include maintaining the security of ICT’s system, conducting data analytics, responding to your communications, managing ICT’s business relationship with you, enhancing, modifying or improving ICT’s services and identifying usage trends. Where required by law and where such personal data is collected via cookies or other similar technologies, ICT otherwise only processes personal data for marketing purposes or analytics on the basis of user **consent**. Note that where consent is relied upon, ICT will not combine this lawful basis with any other, as we recognize this would be inherently unfair to user rights.
- **Cookies:** Our online ordering solution is powered by Shopify and Sparklayer, refer to: <https://www.shopify.com/legal/cookies> and <https://www.sparklayer.io/privacy> for further details.

Salesforce

- **Purpose:** Contact and account data is combined with sales history to effectively manage our customer relationships, quote projects and analyze sales trends.
- **Data:** Names, email addresses, addresses (optional), phone numbers (optional).
- **Method:** Majority of customer data stored is entered by the customer when registering on our website which creates leads in Salesforce. Customer information is occasionally augmented by ZoomInfo matched records.
- **Storage:** Stored in Salesforce's cloud servers (AWS).
- **Hosting Region:** Japan. ICT relies on the adequacy decision and regulation issued by the European Commission and UK Government for transfers from the EEA and UK to this region.
- **Third Parties:** Contact names, company names, titles and email addresses are accessed by DocuSign when account applications and NDAs are generated. This minimizes the time spent filling out forms.
- **Retention:** Personal data is retained only for as long as necessary for the purposes for which it was collected, in accordance with our data retention policy and applicable data protection laws. Users may request deletion of their personal data in accordance with their rights under applicable data protection legislation.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.

Some examples of ICT’s legitimate interests include maintaining the security of ICT’s system, conducting data analytics, responding to your communications, managing ICT’s business relationship with you, enhancing, modifying or improving ICT’s services and identifying usage trends.

- **Cookies:** N/A, no end user access.

Marketing Cloud Account Engagement (MCAE)

- **Purpose:** A marketing automation platform designed to help generate and nurture leads, track engagement, and send marketing emails to subscribed users.
- **Data:** Optional forms can collect user data including email address, name, company name, phone number, region (country, state), job title, user type and query. The user's IP address may be captured when they visit certain web pages containing MCAE tracking codes.
- **Method:** Data is typically submitted directly by users via website forms. Data may also be synced from Salesforce or input directly by administrative users.
- **Storage:** Salesforce cloud servers (AWS).
- **Hosting Region:** USA. Personal data transferred to the United States are processed under the EU-U.S. Data Privacy Framework certification where applicable. For entities not covered by this framework, Standard Contractual Clauses (SCCs), the UK Addendum, and supplementary measures are implemented in accordance with GDPR and UK GDPR requirements.
- **Third Parties:** Data may be synced to Salesforce.
- **Retention:** Data is kept in the system indefinitely unless removed by an administrative user. If the data is synced with a Salesforce record and that Salesforce record is deleted, the MCAE record is automatically deleted.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user's fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user's interests or fundamental rights and freedoms. ICT's legitimate interests relate to ICT's commercial interests and ICT's need to operate business to provide the requested goods and services.

Some examples of ICT's legitimate interests include maintaining the security of ICT's system, conducting data analytics, responding to your communications, managing ICT's business relationship with you, enhancing, modifying or improving ICT's services and identifying usage trends. Where required by law and where such personal data is collected via cookies or other similar technologies, ICT otherwise only processes personal data for marketing purposes or analytics on the basis of user **consent**. Note that where consent is relied upon, ICT will not combine this lawful basis with any other, as we recognize this would be inherently unfair to user rights.
- **Cookies:** Some MCAE forms are embedded in ict.co web pages. See <https://ict.co/privacy-policy/cookie-policy> for further details.

Google Analytics

- **Purpose:** A web analytics tool that tracks and reports website performance, helping to understand user behavior and measure the effectiveness of marketing efforts.
- **Data:** Session data such as the user's device type, browser, operating system, location, traffic source (e.g. search, social, direct), pages viewed, time spent on each page, interactions (e.g. clicks or form submissions) and session behavior, along with anonymized identifiers to track repeat visits and user journeys.
- **Method:** Google Analytics captures data when the user visits the ICT website.
- **Storage:** Google cloud servers.
- **Hosting Region:** USA. Personal data transferred to the United States are processed under the EU–U.S. Data Privacy Framework certification where applicable. For entities not covered by this framework, Standard Contractual Clauses (SCCs), the UK Addendum, and supplementary measures are implemented in accordance with GDPR and UK GDPR requirements.
- **Third Parties:** Google Analytics does not share personally identifiable data with third-party systems; however, aggregated or anonymized data may be used by Google for benchmarking and product improvement.
- **Retention:** Data is retained for 14 months, after which user-level and event-level data are automatically deleted, though aggregated data in reports may remain available indefinitely.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user's fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user's interests or fundamental rights and freedoms. ICT's legitimate interests relate to ICT's commercial interests and ICT's need to operate business to provide the requested goods and services.

Some examples of ICT's legitimate interests include maintaining the security of ICT's system, conducting data analytics, responding to your communications, managing ICT's business relationship with you, enhancing, modifying or improving ICT's services and identifying usage trends. Where required by law and where such personal data is collected via cookies or other similar technologies, ICT otherwise only processes personal data for marketing purposes or analytics on the basis of user **consent**. Note that where consent is relied upon, ICT will not combine this lawful basis with any other, as we recognize this would be inherently unfair to user rights.

- **Cookies:** Refer to <https://ict.co/privacy-policy/cookie-policy>.

Zendesk for Customer Service

- **Purpose:** Issue tracking system used by Customer Services to manage order processing.
- **Data:** Names, email addresses, addresses, phone numbers, product details unique to specific customers, software serial numbers, credential profile identifiers, site names and purchase order numbers.
- **Method:** Data is submitted directly by the user via email. Order-specific data is manually processed and uploaded to SAP for order dispatch.
- **Storage:** Stored in Zendesk cloud servers (AWS).
- **Hosting Region:** Regions include the United States, Ireland and the UK, Germany, Japan and Australia. For countries outside the UK or EEA, and those with an adequacy decision or regulation (e.g. Japan or where the recipient entity is certified under the EU-U.S. Data Privacy Framework and UK Extension), we rely on that decision or regulation or certification. For other countries outside the UK and EEA (e.g. Australia or non-certified U.S. entities), we use the Standard Contractual Clauses (SCCs) and the UK Addendum, along with supplementary measures where required. For transfers between the EEA and the UK, we rely on the reciprocal adequacy findings of the European Commission and UK Government.
- **Third Parties:** N/A
- **Retention:** Personal data is retained only for as long as necessary for the purposes for which it was collected, in accordance with our data retention policy and applicable data protection laws. Users may request deletion of their personal data in accordance with their rights under applicable data protection legislation.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.

Some examples of ICT’s legitimate interests include maintaining the security of ICT’s system, conducting data analytics, responding to your communications, managing ICT’s business relationship with you, enhancing, modifying or improving ICT’s services and identifying usage trends. Where required by law and where such personal data is collected via cookies or other similar technologies, ICT otherwise only processes personal data for marketing purposes or analytics on the basis of user **consent**. Note that where consent is relied upon, ICT will not combine this lawful basis with any other, as we recognize this would be inherently unfair to user rights.
- **Cookies:** No changes have been made to standard settings:
<https://www.zendesk.com/company/agreements-and-terms/cookie-notice/#how-does-zendesk-use-tracking-technologies>

Zendesk for Technical Support

- **Purpose:** Issue tracking system used to track and resolve technical queries for customers.
- **Data:** Names, email addresses, addresses, phone numbers, product details unique to specific customers, software serial numbers, credential profile identifiers, site names and purchase order numbers.
- **Method:** Data is submitted directly by the user via email or via website forms, creating a Zendesk ticket. User data is synced from Salesforce when contact and account records are created or updated. Ticket information is synced to Salesforce.
- **Storage:** Stored in Zendesk cloud servers (AWS).
- **Hosting Region:** Regions include the United States, Ireland and the UK, Germany, Japan and Australia. For countries outside the UK or EEA, and those with an adequacy decision or regulation (e.g. Japan or where the recipient entity is certified under the EU-U.S. Data Privacy Framework and UK Extension), we rely on that decision or regulation or certification. For other countries outside the UK and EEA (e.g. Australia or non-certified U.S. entities), we use the Standard Contractual Clauses (SCCs) and the UK Addendum, along with supplementary measures where required. For transfers between the EEA and the UK, we rely on the reciprocal adequacy findings of the European Commission and UK Government.
- **Third Parties:** Data is synced to linked records in Salesforce.
- **Retention:** Personal data is retained only for as long as necessary for the purposes for which it was collected, in accordance with our data retention policy and applicable data protection laws. Users may request deletion of their personal data in accordance with their rights under applicable data protection legislation.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.

Some examples of ICT’s legitimate interests include maintaining the security of ICT’s system, conducting data analytics, responding to your communications, managing ICT’s business relationship with you, enhancing, modifying or improving ICT’s services and identifying usage trends. Where required by law and where such personal data is collected via cookies or other similar technologies, ICT otherwise only processes personal data for marketing purposes or analytics on the basis of user **consent**. Note that where consent is relied upon, ICT will not combine this lawful basis with any other, as we recognize this would be inherently unfair to user rights.

- **Cookies:** No changes have been made to standard settings:
<https://www.zendesk.com/company/agreements-and-terms/cookie-notice/#how-does-zendesk-use-tracking-technologies>

SAP S/4HANA

- **Purpose:** Cloud-based enterprise resource planning (ERP) system used to manage critical business processes across various departments, including manufacturing, order processing and fulfillment, accounting, procurement and supply chain management.
- **Data:** Names, email addresses, addresses, phone numbers, product details unique to specific customers, software serial numbers, credential profile identifiers, site names, purchase order numbers, financial information, product related information BOMs, product pricing, supplier parts and pricing.
- **Method:** Data is manually processed and uploaded to SAP.
- **Storage:** Stored in SAP managed cloud infrastructure.
- **Hosting Region:** Australia. Where personal data is hosted in Australia, which is not currently recognized by the European Commission or UK Government as providing an adequate level of protection, we implement Standard Contractual Clauses (SCCs) and, where applicable, the UK Addendum, along with supplementary technical and organizational measures in line with EU and UK GDPR requirements.
- **Third Parties:** N/A
- **Retention:** Personal data is retained only for as long as necessary for the purposes for which it was collected, in accordance with our data retention policy and applicable data protection laws. Users may request deletion of their personal data in accordance with their rights under applicable data protection legislation.
- **Lawful Basis:** (i) **Performance of a Contract**—We rely on the contract or agreement which is in force where the processing is necessary to provide the requested ICT products or services; (ii) **Legitimate Interests**—Where ICT processes your personal data on the basis of legitimate interests, and when users are usually resident in the EEA or UK, we have conducted and documented a “legitimate interests impact assessment”, balancing our interests against the user’s fundamental rights and freedoms. We process data only where our legitimate interests are not overridden by a user’s interests or fundamental rights and freedoms. ICT’s legitimate interests relate to ICT’s commercial interests and ICT’s need to operate business to provide the requested goods and services.
Some examples of ICT’s legitimate interests include maintaining the security of ICT’s system, conducting data analytics, responding to your communications, managing ICT’s business relationship with you, enhancing, modifying or improving ICT’s services and identifying usage trends.
- **Cookies:** N/A, no end user access.